全国计算机技术与软件专业技术资格（水平）考试指定用书

网络规划设计师教程

黄传河 主编

全国计算机专业技术资格考试办公室 组编



清华大学出版社

全国计算机技术与软件专业技术资格（水平）考试指定用书

网络规划设计师教程

黄传河　主编

全国计算机专业技术资格考试办公室　组编

清 华 大 学 出 版 社

北　京

内 容 简 介

本书是全国计算机技术与软件专业技术资格（水平）考试的指定用书。依据网络规划设计师考试大纲，本书包含了计算机网络原理、网络规划与设计、网络资源设备、网络安全、标准化与知识产权等内容。本书以实用为主，兼顾基础知识，是参加本考试的必备教材，也可作为网络工程从业人员学习网络技术的教材或日常工作的参考用书。本书也是一本很好的研究生参考用书。

本书扉页为防伪页，封面贴有清华大学出版社防伪标签，无标签者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989　13701121933

图书在版编目(CIP)数据

网络规划设计师教程/黄传河主编；全国计算机专业技术资格考试办公室组编. —北京：清华大学出版社，2009.6
（全国计算机技术与软件专业技术资格（水平）考试指定用书）
ISBN 978-7-302-19932-8

I. 网…　II. ①黄…　②全…　III. 计算机网络-工程技术人员-资格考核-自学参考资料
IV. TP393

中国版本图书馆 CIP 数据核字（2009）第 056980 号

责任编辑：柴文强　薛　阳
责任校对：徐俊伟
责任印制：
出版发行：清华大学出版社　　**地　　址：**北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编：**100084
社 总 机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185×230　**印　张：**54.75　**防伪页：**1　**字　数：**1262 千字
版　　次：2009 年 6 月第 1 版　**印　次：**2009 年 6 月第 1 次印刷
印　　数：
定　　价：　　元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：010-62770177 转 3103　产品编号：033372-01

序　言

软件产业是信息产业的核心之一，是经济社会发展的基础性、先导性和战略性产业，在推进信息化与工业化融合、促进发展方式转变和产业结构升级、维护国家安全等方面有着重要作用。党中央、国务院高度重视软件产业发展，先后出台了 18 号文件、47 号文件等一系列政策措施，营造了良好的发展环境。近年来，我国软件产业进入快速发展期。2007 年销售收入达到 5834 亿元，出口 102.4 亿美元，软件从业人数达 148 万人。全国共认定软件企业超过 1.8 万家，登记备案软件产品超过 5 万个。软件技术创新取得突破，国产操作系统、数据库、中间件等基础软件相继推出并得到了较好的应用。软件与信息服务外包蓬勃发展，软件正版化工作顺利推进。

随着软件产业的快速发展，软件人才需求日益迫切。为适应产业发展需求、规范软件专业人员技术资格，20 余年前全国计算机软件考试创办，率先执行了以考代评政策。近年来，考试作了很多积极的探索，进行了一系列改革，考试名称、考试内容、专业类别、职业岗位也作了相应的变化。目前，考试名称已调整为计算机技术与软件专业技术资格（水平）考试，涉及 5 个专业类别、3 个级别层次共 27 个职业岗位，采取水平考试的形式，执行资格考试政策，并扩展到高级资格，取得了良好效果。20 余年来，累计报考人数近 200 万，影响力不断扩大。程序员、软件设计师、系统分析师、网络工程师、数据库系统工程师的考试标准已与日本相应考试级别实现互认，程序员和软件设计师的考试标准与韩国实现互认。通过考试，一大批软件人才脱颖而出，为加快培育软件人才队伍、推动软件产业健康发展起到了重要作用。

最近，工业和信息化部电子教育与考试中心组织了一批具有较高理论水平和丰富实践经验的专家编写了这套全国计算机技术与软件专业技术资格（水平）考试教材和辅导用书。按照考试大纲的要求，教材和辅导用书全面介绍相关知识与技术，帮助考生学习备考，将为软件考试的规范和完善起到积极作用。

我相信，通过社会各界共同努力，全国计算机技术与软件专业技术资格（水平）考试将更加规范、科学，培养出更多专业技术人才，为加快发展信息产业、推动信息化与工业化融合做出积极贡献。

工业和信息化部副部长　娄勤俭

前　言

计算机网络是信息传输、收集、存储、处理、分配、消费的最重要的载体，是网络经济的核心，深刻地影响着经济、社会、文化、科技，是工作和生活的最重要工具之一。

网络规划设计师的职责就是规划、设计、并指导实施网络工程，为人们提供高速、可靠、经济、安全、方便的网络，满足人们的需要。因此，网络规划设计师应熟悉应用领域的业务，能够进行计算机网络领域的需求分析、规划设计、部署实施、评测运维等工作。具体来说，就是在需求分析阶段，能分析用户的需求和约束条件，写出网络系统需求规格说明书；在规划设计阶段，能根据系统需求规格说明书，完成逻辑结构设计、物理结构设计，选用适宜的网络设备，按照标准规范编写系统设计文档及项目开发计划；在部署实施阶段，能按照系统设计文档和项目开发计划组织项目施工，对项目实施过程进行质量控制、进度控制、经费控制，能具体指导项目实施；在评测运维阶段，能根据相关标准和规范对网络进行评估测试，能制定运行维护、故障分析与处理机制，确保网络提供正常服务；能指导制定用户的数据和网络战略规划，能指导网络工程师进行系统建设实施。

本书以系统观点，按网络要素组织网络知识体系，将网络规划设计师应具备的网络知识划分为五大部分，分别加以介绍。另外，增加两章介绍与考试相关的内容。

第 1 章介绍网络的基本原理，第 2 章介绍网络规划设计的知识和方法，第 3 章介绍网络设备和网络软件，第 4 章介绍网络安全技术，第 5 章介绍标准化与知识产权。第 6 章和第 7 章是帮助读者参加考试的内容，第 6 章介绍几个网络规划设计案例，第 7 章介绍论文写作的注意事项。

本书由黄传河规划、统编、审定，吴产乐担任顾问和指导。参加编写的有（按姓名拼音顺序）：陈晶（4.2、4.7）、杜瑞颖（1.4、1.7、1.8）、黄传河（1.1、1.5）、吕慧（1.2）、彭国军（4.1）、石岗（第 3 章）、涂航（4.8～4.11）、吴黎兵（4.3、4.5、4.6、第 6 章）、余纯武（4.12～4.15）、张春林（1.3、1.6、第 7 章）、张沪寅（1.9、1.10）、张健（2.1～2.6）、张萌（2.7、2.8）、张文涛（4.4、第 5 章）。

由于时间仓促，书中难免有不妥、错误之处，敬请指正。

作　者
2009 年 3 月于珞珈山

目　录

第 1 章　计算机网络原理

计算机网络是计算机技术与通信技术相结合的产物。计算机网络是信息收集、分配、存储、处理、消费的最重要的载体，是网络经济的核心，深刻地影响着经济、社会、文化、科技，是工作和生活的最重要工具之一。掌握网络的基本原理是进行网络规划与设计的基础。本章从网络概述、数据通信基础知识、网络体系结构、网络设备与网络软件、局域网、广域网与接入网、网络互联、Internet 协议、网络管理、网络服务质量等方面介绍计算机网络的原理。

1.1　计算机网络概论

1.1.1　计算机网络概念

1．计算机网络的定义

计算机网络是一个将分散的、具有独立功能的计算机系统，通过通信设备与线路连接起来，由功能完善的软件实现资源共享的系统。

对于这一说法，其中仍有一些不确定的地方，如完善的标准是什么？资源共享的内容、方式、程度是什么？资源共享是最终目标吗？鉴于这些不确定性，对计算机网络的理解主要有三种观点：

（1）广义观点。持此观点的人认为，只要是能实现远程信息处理的系统或进一步能达到资源共享的系统都可以成为计算机网络。

（2）资源共享观点。持此观点的人认为，计算机网络必须是由具有独立功能的计算机组成的、能够实现资源共享的系统。

（3）用户透明观点。持此观点的人认为，计算机网络就是一台超级计算机，资源丰富、功能强大，其使用方式对用户透明，用户使用网络就像使用单一计算机一样，无需了解网络的存在、资源的位置等信息。这是最高标准，目前还未实现，是网络未来发展追求的目标。

计算机网络的应用越来越广泛，深刻地影响着社会发展的进程。今天要列数哪里不需要计算机网络已经变得非常困难。在此我们只简单地说明计算机网络的几个应用方向。

- 对分散的信息进行集中、实时处理。比如航空订票系统、工业控制系统、军事系统等众多的系统，离开了计算机网络，将无法进行。
- 共享资源。实现对各类资源的共享，包括信息资源、硬件资源、软件资源。网格

是计算机网络的高级形态，将使资源共享变得更加方便、透明。

- 电子化办公与服务。借助计算机网络，得以实现电子政务、电子商务、电子银行、电子海关等一系列借助计算机网络实现的现代化办公、商务应用。当今社会，就连到商场购物、餐馆吃饭这样的日常事务都离不开计算机网络。利用计算机网络进行网上购物，更加方便、廉价。
- 通信。电子邮件、即时通信系统等众多的通信功能，极大地方便了人与人之间的信息交往，既快速又廉价。
- 远程教育。利用网络可以提供远程教育平台，借助丰富的知识管理系统，学生可以更加方便地自学，提高学习效率。
- 娱乐。娱乐是人的天性，对于大多数人来说，工作之余都需要娱乐活动来丰富自己的生活。利用网络提供各种各样的娱乐内容，既满足了社会的需要，同时也具有巨大的经济效益。

2．计算机网络与通信、网络的关系

通信（communication）就是信息的传递，是指由一地向另一地进行信息的传输与交换，其目的是传输消息。实现通信功能的系统称为通信系统。

随着社会的发展，人们对传递消息的要求也越来越高。在各种各样的通信方式中，利用“电”来传递消息的通信方法称为电信（telecommunication），这种通信具有迅速、准确、可靠等特点，且几乎不受时间、地点、空间、距离的限制，因而得到了飞速发展和广泛应用。

以语音通信为主要目的建立的通信系统统称为电话网络或电信网络，包括固话网络、移动网络等。

以发送电视信号为目的建立的通信系统称为电视网络。

以数据通信为目的建立的网络称为数据通信网络。

计算机网络是计算机技术、通信技术相结合的产物，可实现数据的传输、收集、分配、处理、存储、消费。数据通信网络是计算机网络的基础或初级形式。

现在所说的网络，广义地泛指上述网络之一或全部，狭义地特指计算机网络。

随着技术的进步和应用的相互渗透，电信网络、电视网络、计算机网络将逐步实现三网融合，走向统一。

1.1.2 计算机网络组成

1.1.2.1 计算机网络物理组成

从物理构成上看，计算机网络包括硬件、软件、协议三大部分。

1．硬件

① 两台以上的计算机及终端设备，统称为主机（host），其中部分 host 充当服务器，

部分 host 充当客户机。

② 前端处理机（FEP）或通信处理机或通信控制处理机（CCP），负责发送、接收数据，最简单的 CCP 是网卡。

③ 路由器、交换机等连接设备，交换机将计算机连接成网络，路由器将网络互联组成更大的网络。

④ 通信线路，具体完成将信号从一个地方传送到另一个地方，包括有线线路和无线线路。

2．软件

主要有实现资源共享的软件、方便用户使用的各种工具软件。

3．协议

协议由语法、语义和时序三部分构成。其中语法部分规定传输数据的格式，语义部分规定所要完成的功能，时序部分规定执行各种操作的条件、顺序关系等。协议是计算机网络的核心。一个完整的协议应完成线路管理、寻址、差错控制、流量控制、路由选择、同步控制、数据分段与装配、排序、数据转换、安全管理、计费管理等功能。

1.1.2.2　计算机网络功能组成

从功能上，计算机网络由资源子网和通信子网两部分组成。其中资源子网完成数据的处理、存储等功能，通信子网完成数据的传输功能。资源子网相当于计算机系统，通信子网是为了连网而附加上去的通信设备、通信线路等，如图 1-1 所示。

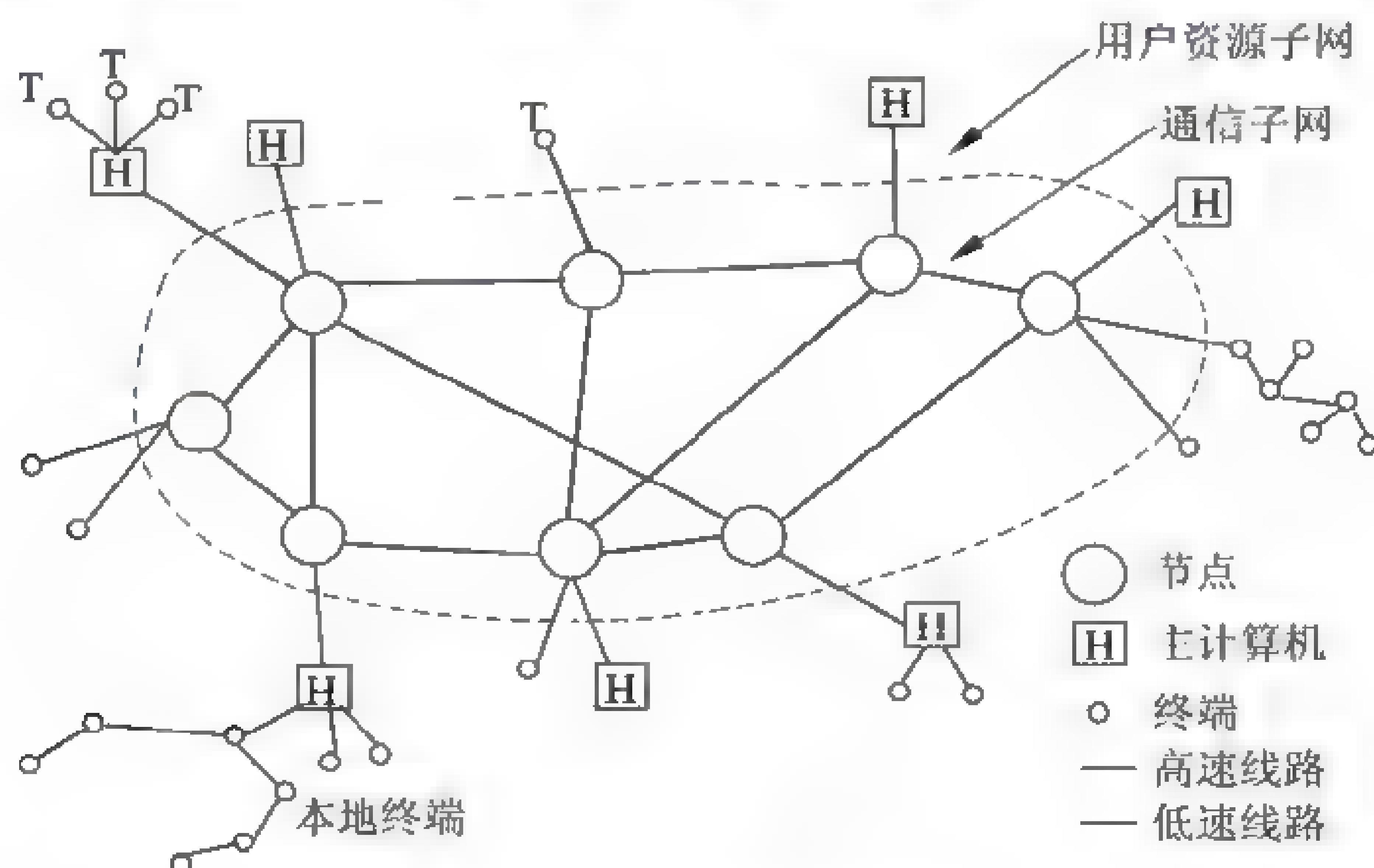


图 1-1　资源子网与通信子网

从工作方式上看，也可以认为计算机网络由边缘部分和核心部分组成。其中边缘部分是用户直接使用的主机，核心部分由大量的网络及路由器组成，为边缘部分提供连通性和交换服务，如图 1-2 所示。

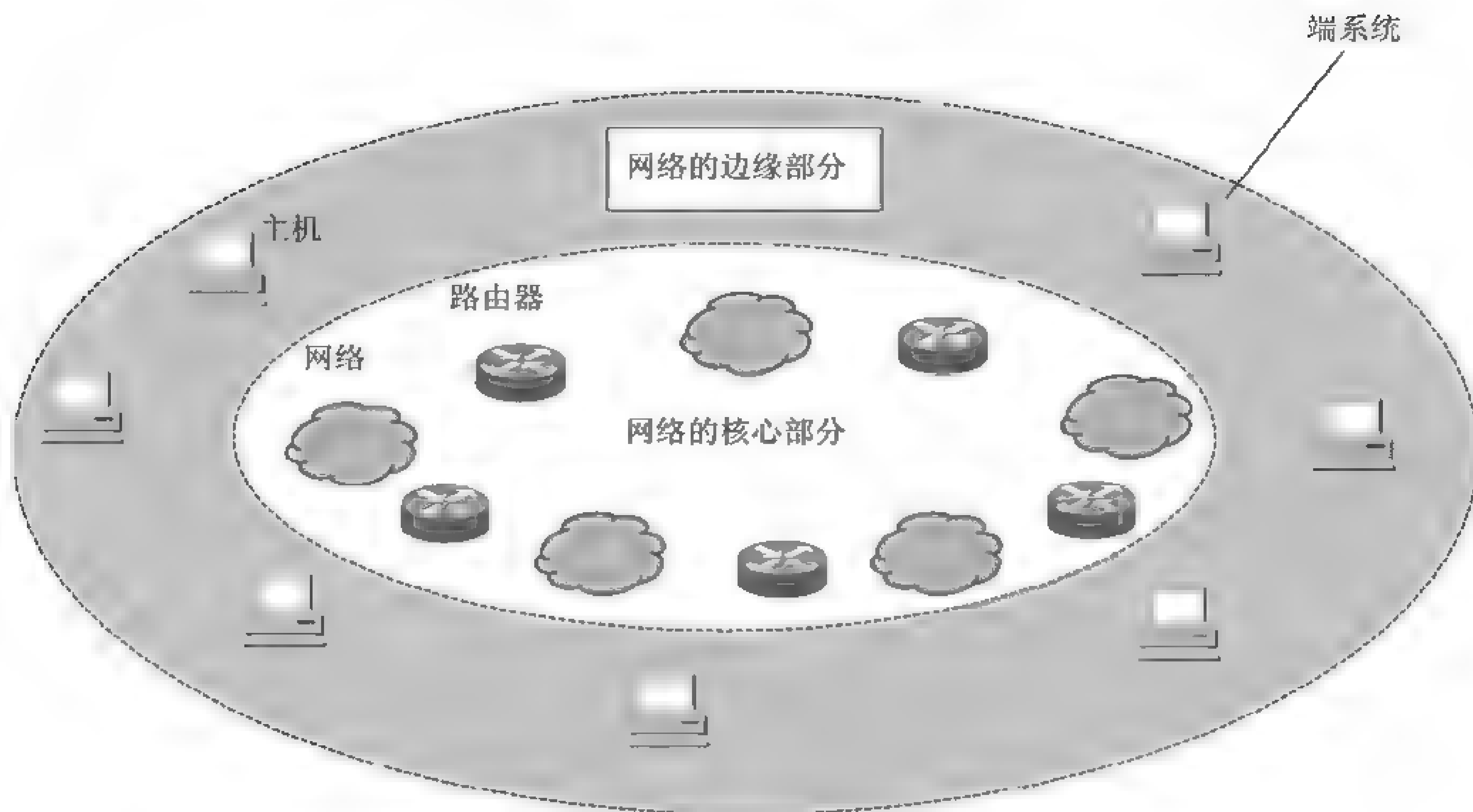


图 1-2　网络的边缘部分与核心部分

1.1.2.3　计算机网络要素组成

从组成要素上看，计算机网络包括计算机、路由器、交换机、网卡、通信线路、调制解调器等基本要素组成。其中计算机包括客户机和服务器，网卡附在计算机里面（也有外接的如 USB 接口网卡），负责与通信线路相连，完成收发工作，交换机用于把小范围内的计算机连接成网络，路由器用于互联多个网络组成更大的网络。调制解调器并不是在任何网络中都需要，其作用是将孤立的计算机连接到网络上。调制解调器有音频调制解调器、ADSL 调制解调器、卫星调制解调器等多种。

1.1.3　计算机网络分类

1．按分布范围分类

按分布范围可将计算机网络分为广域网、城域网、局域网和个域网。

- 广域网（WAN）一般分布在数十公里以上区域。
- 城域网（MAN）一般分布在一个城区，一般使用广域网的技术，可以看成是一个较小的广域网。
- 局域网（LAN）一般分布在几十米到几千米范围，传统上，局域网与广域网使用不同的技术，广域网使用交换技术，局域网使用广播技术，而这才是二者的根本区别。但从万兆以太网开始，这种区别已经消除了。

- 个域网（PAN）一般指家庭内甚至是个人随身携带的网络，一般分布在几米范围内，用于将家用电器、消费电子设备、少量计算机设备连接成一个小型的网络，以采用无线通信方式为主。

2．按拓扑结构分类

按拓扑结构可将计算机网络分为总线型网络、星型网络、环型网络、树型网络、网格型网络等基本形式。

- 总线型网络：用单总线把各计算机连接起来，如图 1-3 所示。总线型网络的优点是建网容易，增减节点方便，节省线路。缺点是重负载时通信效率不高。
- 星型网络：每个终端或计算机都以单独（专用）的线路与一中央设备相连，如图 1-4 所示。中央设备早期是计算机，现在一般是交换机或路由器。星型网络的优点是结构简单，建网容易，延迟小，便于管理。缺点是成本高，中心节点对故障敏感。

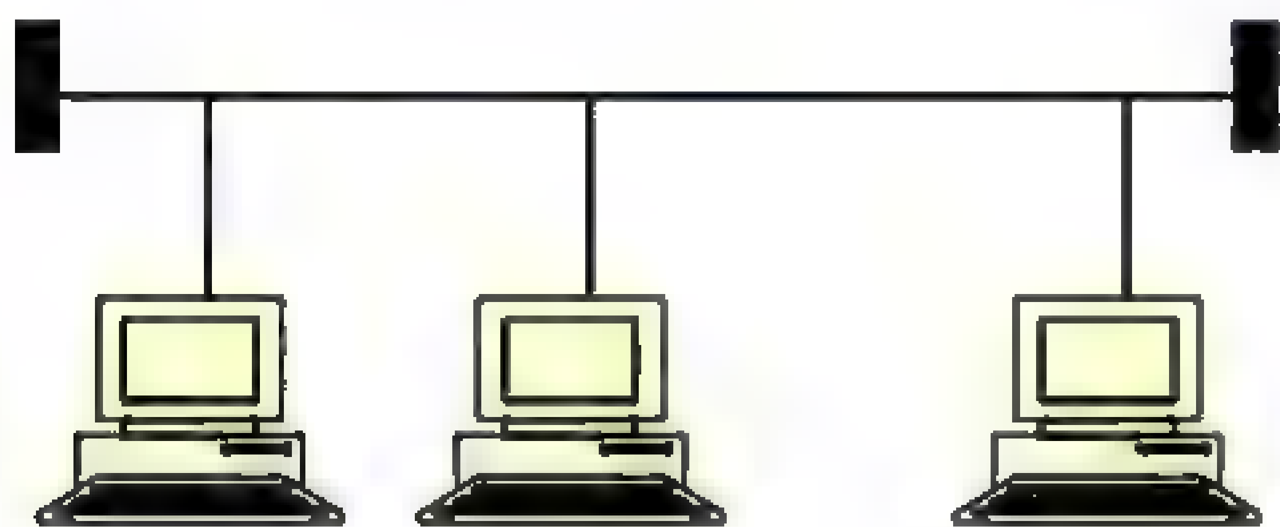


图 1-3　总线型网络

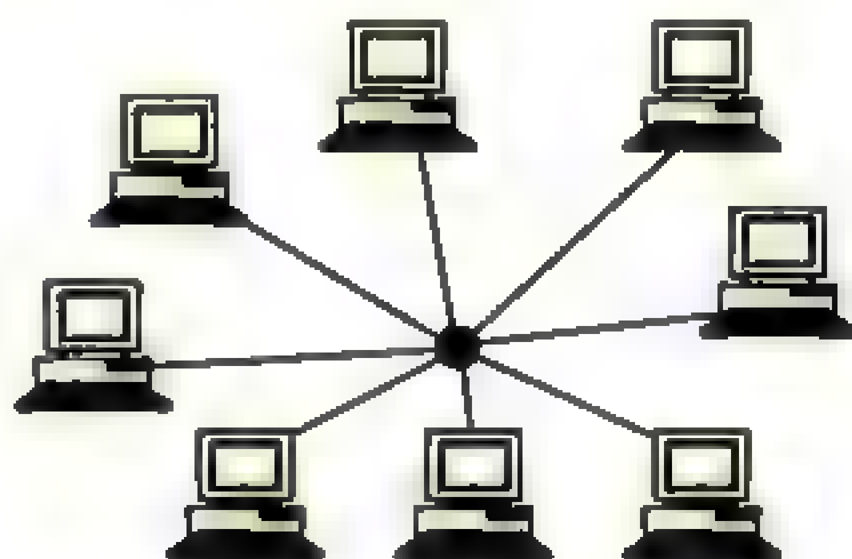


图 1-4　星型网络

- 环型网络：所有计算机环接口设备连接成一个环，可以是单环，也可以是双环。环中信号是单向传输的。双环网络中两个环上信号的传输方向相反，具备自愈功能。
- 树型网络：节点组织成数状结构，具有层次性。
- 网格型网络：一般情况下，每个节点至少有两条路径与其他节点相连。有规则型和非规则型两种。网格型网络的优点是可靠性高，缺点是控制复杂，线路成本高。

可以将这些基本型网络互联组织成更为复杂的网络。

3．按交换技术分类

按交换技术可将网络分为线路交换网络、报文交换网络、分组交换网络等类型。

- 线路交换网络：在源节点和目的节点之间建立一条专用的通路用于数据传送。包括建立连接、传输数据、断开连接三个阶段。最典型的线路交换网络就是电话网络。该类网络的优点数据直接传送延迟小。缺点是线路利用率低，不能充分利用线路容量，不便于进行差错控制。
- 报文交换网络：将用户数据加上源地址、目的地址、长度、校验码等辅助信息封

装成报文，发送给下个节点。下个节点收到后先暂存报文，待输出线路空闲时再转发给下个节点，重复这一过程直到到达目的节点。每个报文可单独选择到达目的节点的路径。这类网络也称为存储-转发网络。其优点是：① 可以充分利用线路容量（可以利用多路复用技术，利用空闲时间）；② 可以实现不同链路之间不同数据率的转换；③ 可以实现一对多、多对一的访问，这是 Internet 的基础；④ 可以实现差错控制；⑤ 可以实现格式转换。缺点是：① 增加资源开销，例如辅助信息导致时间和存储资源开销；② 增加缓冲延迟；③ 多个报文的顺序可能发生错误，需要额外的顺序控制机制；④ 缓冲区难于管理，因为报文的大小不确定，接收方在接收到报文之前不能预知报文的大小。

- 分组交换网络：也称包交换网络，其原理是将数据分成较短的固定长度的数据块，在每个数据块中加上目的地址、源地址等辅助信息组成分组（包），按存储转发方式传输。除具备报文交换网络的优点外，还具有自身的优点：① 缓冲区易于管理；② 包的平均延迟更小，网络中占用的平均缓冲区更少；③ 更易标准化；④ 更适合应用。现在的主流网络基本上都可以看成是分组交换网络。

4. 按采用协议分类

每层的协议都不同，因此按协议的分类应指明协议的区分方式。比如按网络层的关键协议来分类，可以分为 IP 网、IPX 网等，无线网络可以分为 Wi-Fi 网络、蓝牙网络等。

5. 按使用传输介质分类

按传输介质可以分为有线网络和无线网络两大类。有线网络又可以分为双绞线网络、同轴电缆网络、光纤网络、光纤同轴混合网络等。无线网络又可分为无线电、微波、红外等类型。

6. 按用户与网络的关联程度分

按用户与网络的关联程度可以将计算机网络分为骨干网、接入网和驻地网。

1.1.4 网络体系结构

1.1.4.1 分层与体系结构

网络体系结构是指构成计算机网络的各组成部分及计算机网络本身所必须实现的功能的精确定义。更直接地说，是计算机网络中的层次、各层的协议以及层间的接口的集合。

网络非常复杂，为便于研究和实现，需要按体系结构的方式进行建模。而体系结构通常都具有可分层的特性，因此网络体系结构都分成层次结构。

分层的基本原则如下：

① 各层之间界面清晰自然，易于理解，相互交流尽可能少。

② 各层功能的定义独立于具体实现的方法。

③ 保持下层对上层的独立性，单向使用下层提供的服务。

依据上述原则，将网络分成多个层次，从最低层到最高层依此称为第 1 层、第 2 层，……，第 n 层，通常还为每层起一个特定的名称，如第 1 层的名称为物理层。

每层有完成给定功能的实体组成，第 n 层的实体可记为 n-实体。

1.1.4.2　接口、协议与服务

接口是指同一系统内部两个相邻层次之间的交往规则。

协议是指通信双方实现相同功能的相应层之间的交往规则。协议由语法、语义和时序三部分构成。

协议与接口的关系如图 1-5 所示。

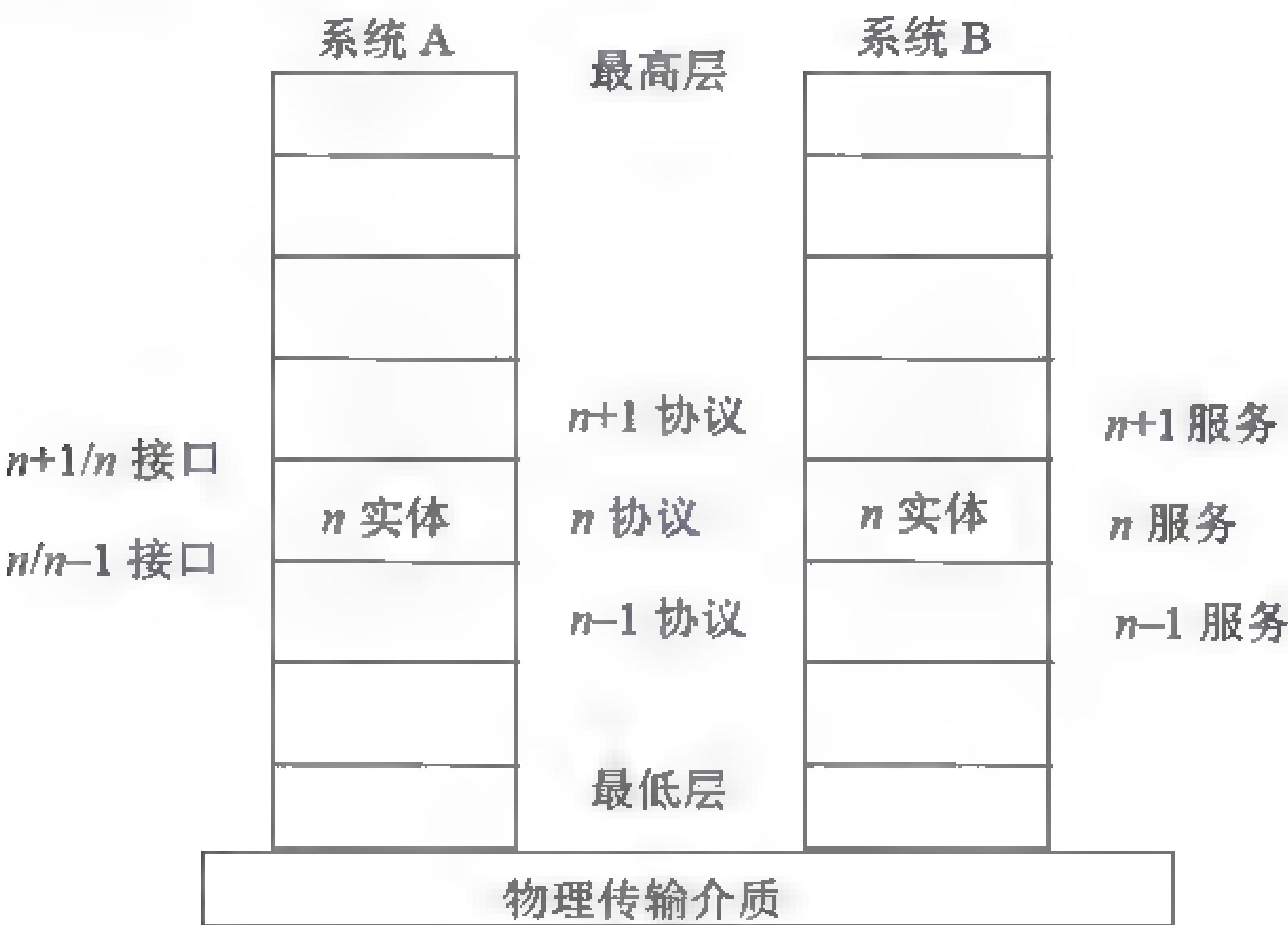


图 1-5　接口与协议

服务是指为紧相邻的上层提供的功能调用，每层只能调用紧相邻的下层提供的服务。服务通过服务访问点（SAP）提供，如图 1-6 所示。

计算机网络提供的服务可分为三类。

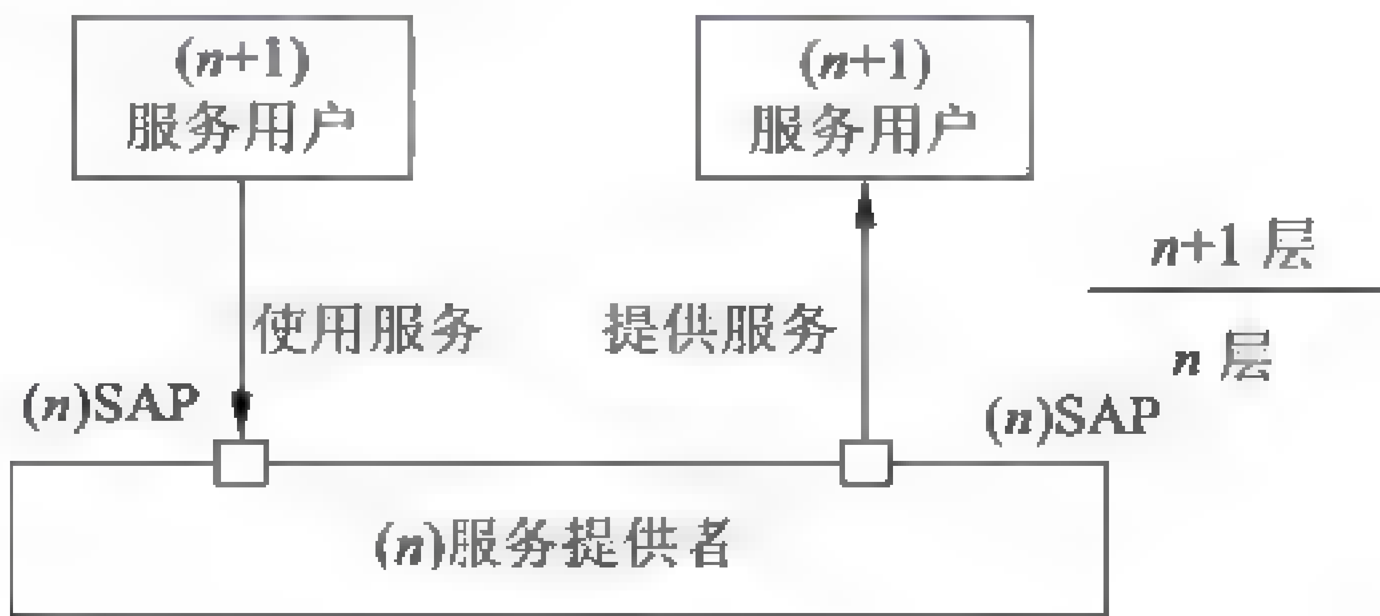


图 1-6　服务及服务访问点

1．面向连接的服务与无连接的服务

面向连接的服务是指在通信之前，双方需先建立连接，然后才能开始传送数据，传送完成后需释放连接。建立连接时需要分配相应的资源如缓冲区，以保证通信能正常进行。比如打电话就是面向连接的服务。无连接的服务是指双方通信前不事先建立连接，需要发送数据时，直接发送。 比如平常写信交由邮局投递的过程就是无连接的服务。

2．有应答服务与无应答服务

有应答服务是指接收方在收到数据后向发送方给出相应的应答，该应答由传输系统内部自动实现，而不是用户实现。例如文件传输服务。

无应答服务是指接收方收到数据后不自动给出应答。若需应答，由高层实现。例如WWW 服务，客户端收到服务器发送的页面文件后不给出应答。

3．可靠服务与不可靠服务

可靠服务是指网络具有检错、纠错、应答机制，能保证数据正确、可靠地传送到目的地。而不可靠服务是指网络不能保证数据正确、可靠地传送到目的地，网络只是尽量正确、可靠，是一种尽力而为的服务。

1.1.4.3 数据传送单位

服务数据单元 SDU：为完成用户所要求的功能而应传送的数据。第 N 层的服务数据单元记为 N-SDU。

协议控制信息 PCI：控制协议操作的信息。第 N 层的协议控制信息记为 N-PCI。

协议数据单元 PDU：协议交换的数据单位。第 N 层的协议数据单元记为 N-PDU。

三者之间的关系为：N-SDU+N-PCI=N-PDU=(N–1)SDU。其变换过程如图 1-7 所示。

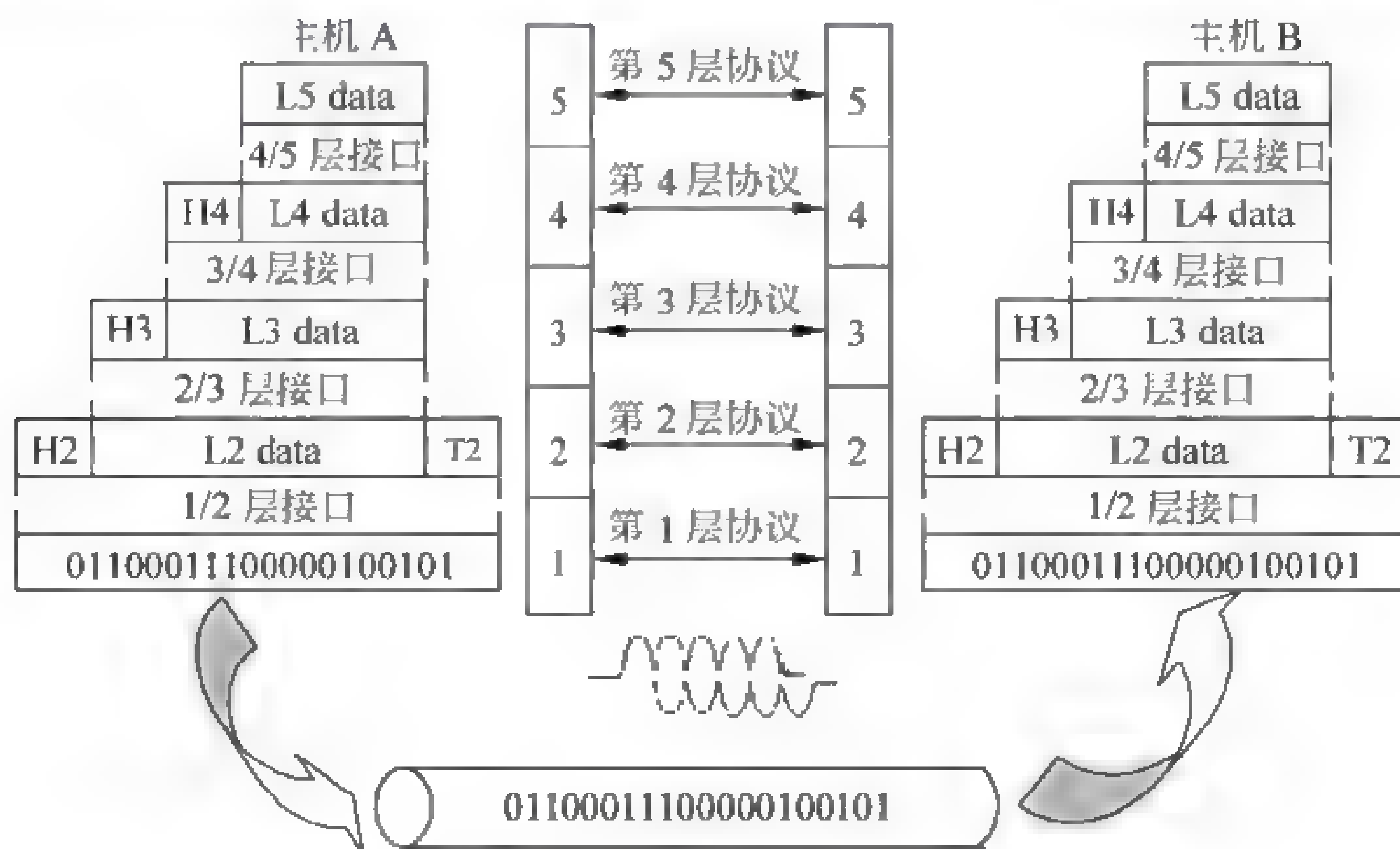


图 1-7 数据单元关系

1.1.4.4　OSI/ISO 与 TCP/IP 体系结构模型

1. OSI 模型

国际标准化组织（International Standardization Organization，ISO）于 1978 年提出了一个网络体系结构模型，称为开放系统互联参考模型（OSI）。OSI 有 7 层，从低到高依次称为物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。如图 1-8 所示。

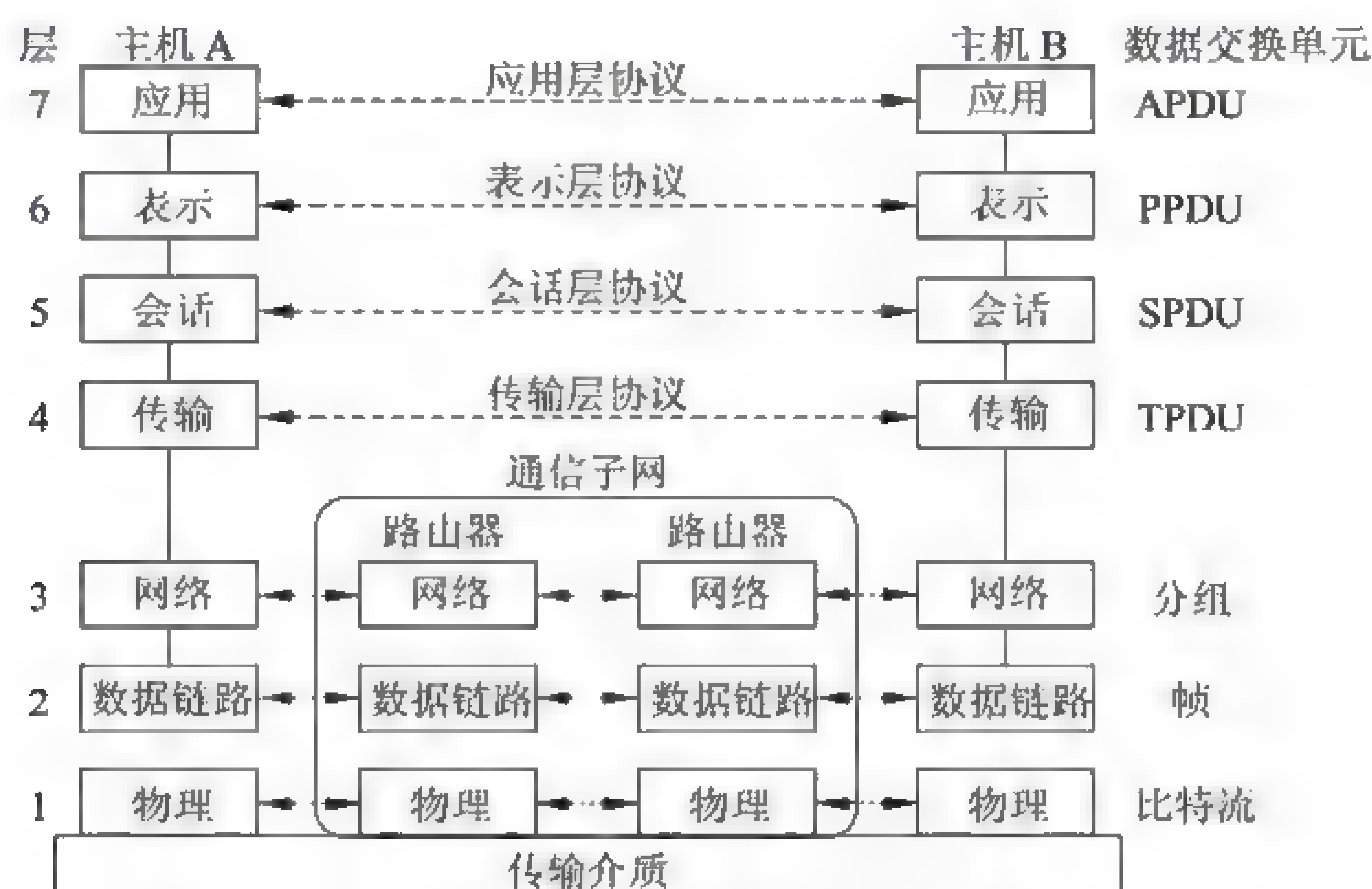


图 1-8　OSI 层次结构

OSI 参考模型中各层的功能如下。

物理层：在链路上透明地传输位。需要完成的工作包括线路配置、确定数据传输模式、确定信号形式、对信号进行编码、连接传输介质。为此定义了建立、维护和拆除物理链路所具备的机械特性、电气特性、功能特性以及规程特性。

数据链路层：把不可靠的信道变为可靠的信道。为此将比特组成帧，在链路上提供点到点的帧传输，并进行差错控制、流量控制等。

网络层：在源节点 目的节点之间进行路由选择、拥塞控制、顺序控制、传送包，保证报文的正确性。网络层控制着通信子网的运行，因而它又称为通信子网层。

传输层：提供端 端间可靠的、透明的数据传输，保证报文顺序的正确性、数据的完整性。

会话层：建立通信进程的逻辑名字与物理名字之间的联系，提供进程之间建立、管理和终止会话的方法，处理同步与恢复问题。

表示层：实现数据转换（包括格式转换、压缩、加密等），提供标准的应用接口、公用的通信服务、公共数据表示方法。

应用层：对用户不透明的各种服务，如 E-mail。

OSI 模型比较完整，但也非常复杂。除了低三层有实现外，其余层次没有实现，现在已基本不用。

2. TCP/IP 模型

美国国防部高级研究计划局（DOD-ARPA）1969 年在研究 ARPANET 时提出了 TCP/IP 模型，从低到高各层依次为网络接口层、互联网层、传输层、应用层，如图 1-9 所示。

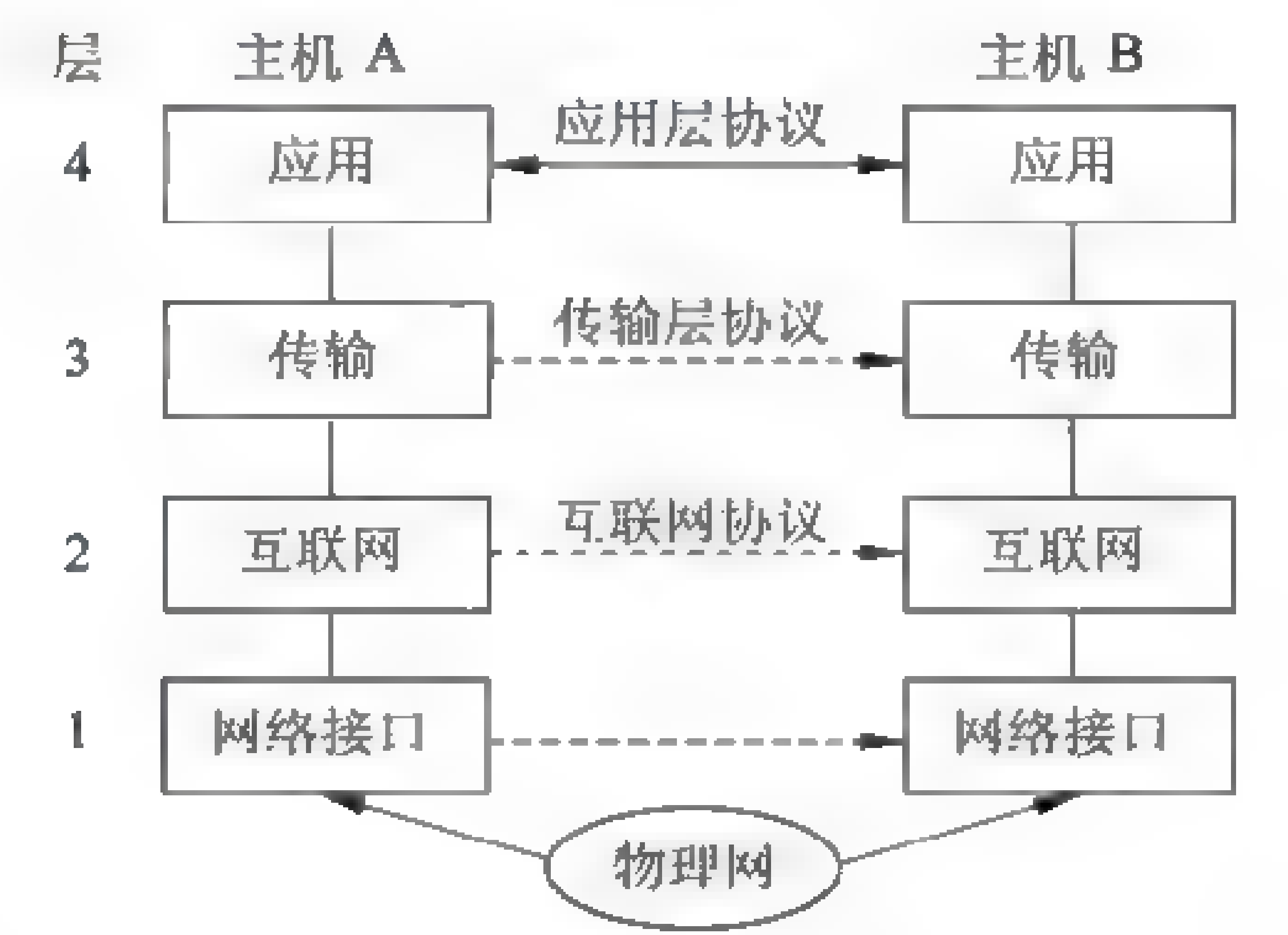


图 1-9　TCP/IP 层次结构

应用层、传输层、互联网层都定义了相应的协议和功能，但网络接口层一直没有明确地定义其功能、协议和实现方式。

应用层的主要协议有 DNS，HTTP，SMTP，POP3，FTP，TELNET，SNMP。

传输层的主要协议有 TCP，UDP。

互联网层的主要协议有 IP，ICMP，ARP，RARP。

TCP/IP 模型与 OSI 模型的大致对应关系如表 1-1 所示。

由于 TCP/IP 有大量的协议和应用支持，现在已成为事实上的标准。

表 1-1　OSI 模型与 TCP/IP 模型对比

<table>
<tr><th>OSI 模型</th><th>TCP/IP 模型</th><th>OSI 模型</th><th>TCP/IP 模型</th></tr>
<tr><td>应用层</td><td>应用层</td><td>网络层</td><td>互联网层</td></tr>
<tr><td>表示层</td><td rowspan="2">不存在</td><td>数据链路层</td><td rowspan="3">网络接口层</td></tr>
<tr><td>会话层</td><td rowspan="2">物理层</td></tr>
<tr><td>传输层</td><td>传输层</td></tr>
</table>

1.2　数据通信基础

1.2.1　数据通信概念

广义地讲，把由一地向另一地或多地进行消息的有效传递称为数据通信。例如两个人在一起聊天，是通过声音来传递消息的，聋哑人之间的手语，是通过手势来传递消息的，只不过通信距离较短；而打电话、发电子邮件等，则分别是通过电话系统和计算机网络来传递消息的，通信距离可以很长。自从 19 世纪末人们开始利用电信号传递消息以来，电信这种通信方法得到了深入研究和飞速发展，形成了一整套完备的理论、技术及相应的设备，成为当今社会最重要的通信手段。所以，从狭义的角度讲，把利用电磁波、电子技术、光电子等手段，借助电信号或光信号实现从一地向另一地或多地进行消息地有效传递和交换的过程称为数据通信。

通信的实质就是实现信息的有效传递，它不仅要将有用的信息进行无失真、高效率的传输，而且还要在传输的过程中减少或消除无用信息和有害信息。

1.2.1.1　基本概念

1．数据和信号

数据是运送信息的实体，而信号则是数据的电气的或电磁的表现。无论数据或信号，都既可以是模拟的也可以是数字的。所谓“模拟的”就是连续变化的，而“数字的”就表示取值仅允许为有限的几个离散数值。

2．信道

信道一般用来表示向某一个方向传送信息的媒体，因此，一条通信电路往往包含一条发送信道和一条接收信道。从通信的双方信息交互的方式看，可以有三种基本方式。

1）单工通信

单工通信只有一个方向的通信而没有反方向的交互，仅需要一条信道，无线电广播、电视广播就属于这种类型。

2）半双工通信

半双工通信即通信的双方都可以发送信息，但不能同时发送。

3）全双工通信

全双工通信即通信的双方可以同时发送和接收信息，通常需要两条信道。

3．码元

数字通信中对数字信号的计量单位采用码元这个概念。一个码元指的是一个固定时长的数字信号波形，该时长称为码元宽度。

4. 传输速率

数字通信系统的传输有效程度可以用码元传输速率和信息传输速率来描述。

1）码元传输速率

码元传输速率又可称为码元速率、信号速率、符号速率、波形速率等，它表示单位时间内数字通信系统所传输的码元个数（符号个数或脉冲个数），单位是波特（Baud）。1 波特表示数字通信系统每秒传输 1 个码元。这里的码元可以是多进制的，也可以是二进制的。

2）信息传输速率

信息传输速率又可称为信息速率、比特率等，它表示单位时间内数字通信系统传输的二进制码元个数，单位是比特/秒（bps）。

5. 抖动

所谓抖动，是指在噪声因素的影响下，数字信号的有效瞬间相对于应生成理想时间位置的短时偏离，是数字通信系统中数字信号传输的一种不稳定现象，也即数字信号在传输过程中，造成的脉冲信号在时间间隔上不再是等间隔的，而是随时间变化的。

抖动是由于噪声、定时恢复电路调谐不准、系统复用设备的复用和分路过程中引入的时间误差，以及传输信道质量变化等多种因素引起的。当有多个中继站时，抖动会产生累积，对数字传输系统产生影响，因此，一般都有规定的限度。抖动容限一般用峰-峰抖动来描述，它是指某个特定的抖动比特的时间位置相对于该比特抖动时的时间位置的最大部分偏离。设数字脉冲一比特宽度为 T，偏离位置用$\Delta\tau$表示，则

$$\text{抖动容限}=\frac{\Delta\tau}{T}\times 100\%$$

1.2.1.2 传输指标

通常需要对网络的效率和性能进行衡量，因此了解各种影响网络性能的传输指标是很重要的。

1. 带宽

在过去，通信的主干线路都用来传送模拟信号，一个特定的信号通常是由许多不同的频率成分组成的，因此，一个信号的带宽是指该信号的各种不同频率成分所占据的频率范围，也就是说，带宽本来是指某个信号具有的频带宽度，单位是赫。

当通信线路用来传送数字信号时，数据率就应当成为数字信道最重要的指标。但习惯上，人们愿意将“带宽”作为数字信道所能传送的“最高数据率”的同义词。因此，网络的带宽是指在一段特定的时间内网络所能传送的比特数，单位是比特每秒。例如，一个网络带宽为 10Mbps，意味着每秒能传送 1 千万个比特。

正因为带宽代表数字信号的发送速率，因此带宽有时也称为吞吐量（throughput）。实际应用中，吞吐量常用每秒发送的比特数（或字节数、帧数）来表示。

2．时延

时延是指一个报文或分组从一个网络一端传到另一端所需的时间。通常，时延由三个部分组成。

1）发送时延

发送时延又称为传输时延，是节点在发送数据时使报文或分组从节点进入到传输媒体所需要的时间，也就是从报文或分组的第一个比特开始发送算起，到最后一个比特发送完毕所需的时间。它的计算公式是：

$$发送时延=\frac{报文或分组长度}{信道带宽}$$

信道带宽是指数据在信道上的发送速率，也常称为数据在信道上的传输速率。

2）传播时延

传播时延是电磁波在信道中需要传播一定的距离而花费的时间，其计算公式是：

$$传播时延=\frac{信道长度}{电磁波在信道上的传播速率}$$

电磁波在自由空间的传播速率是光速，即 3.0×10^5km/s。电磁波在网络传输媒体中的传播速率比在自由空间要略低一些，在铜线中的传播速率约为 2.3×10^5km/s，在光纤中的传播速率约为 2.0×10^5km/s。

3）处理时延

处理时延是数据在交换节点为存储转发而进行一些必要的处理所花费的时间。处理时延重要的组成部分是分组在节点缓存队列中排队所经历的排队时延，因此，处理时延的长短通常取决于网络中当时的通信量，当网络的通信量大时，还会发生队列溢出，使分组丢失，这相当于处理时延为无穷大。

这样，数据经历的总时延就是以上三种时延之和：

$$总时延=传播时延+发送时延+处理时延$$

在计算机网络中，往返时延（Round-Trip Time，RTT）也是一个重要的性能指标，它表示从发送方发送数据开始，到发送方收到来自接收方的确认，总共经历的时延。对于复杂的网络，往返时延要包括各中间节点的处理时延和转发数据时的发送时延。

当客户实现新的数字语音和视频应用时，可能更关心时延变化。时延变化通常与端到端或者往返时延一起，对应用的性能需求进行全面的描述。当用户对信息的两次获得的时间间隔较为敏感时，就需要用时延变化来描述性能。

3．时延带宽积

将网络性能的传播时延和带宽两个基本度量相乘，就得到另一个有用的度量：时延带宽积，即

$$时延带宽积=传播时延\times带宽$$

直观地说，如果将一对进程之间的信道看成一条中空的管道，时延相当于管道的长

度，带宽相当于管道的直径，如图 1-10 所示，那么时延带宽积就是管道的容积，即它所能容纳的比特数。



图 1-10 将网络看作一个管道

构造高性能网络时知道时延带宽积是很重要的，因为它相当于第一个比特到达接收方之前，发送方最多发送的比特数。如果发送方希望接收方给出比特已经开始到达的信号，而且这个信号发回到发送方需要经过另一信道时延，那么发送方在接收到到达信号之前能够发完 2 倍时延带宽积的数据。另一方面，如果发送方没有填满管道，即它停下来等到达信号，那么发送方就不能充分利用网络。

4．误码率

在数字通信中是用脉冲信号携带信息，由于噪声、串音、码间干扰以及其他突发因素的影响，当干扰幅度超过脉冲信号再生判决的某一门限值时，将会造成误判而成为误码。误码用误码率来表征，它指在一定统计时间内，数字信号在传输过程中发生错误的位数与传输的总位数之比，用符号 P_e 表示：

$$P_e = \lim_{n\to\infty}\frac{错误位数}{传输的总位数}$$

1.2.1.3 数字传输与模拟传输

按承载消息的电信号形式的不同，通信可分为模拟传输和数字传输。

模拟传输是指以模拟信号来传输消息的通信方式。当信号的某一参量可以取无限多个数值，且直接与消息相对应时，称为模拟信号。

数字传输是指用数字信号来传送消息的通信方式。当信号的某一参量只能取有限个数值，且常常不直接与消息相对应时，称为数字信号，有时也称为离散信号。

不论是数字数据还是模拟数据，都可以采用两种传输方式之一进行传输。

数字数据（二进制序列）→编码为数字信号→数字传输

数字数据（二进制序列）→调制为模拟信号（MODEM）→模拟传输

模拟数据（连续值）→编码为数字信号（CODEC）→数字传输

模拟数据（二进制序列）→调制为模拟信号→模拟传输

1.2.1.4　基带传输与频带传输

基带传输是指信号没有经过调制而直接送到信道中去传输的一种方式，采用这种信号传输技术的通信系统称为基带传输通信系统，简称基带系统。频带传输是指信号经过调制后再送到信道中传输的一种方式，接收端要进行相应的解调才能恢复原来的信号，采用这种信号传输技术的通信系统称为频带传输通信系统，简称频带系统。

1.2.1.5　传输损害

由于各种的传输损害，任何通信系统接收到的信号和发送的信号会有所不同。对模拟信号而言，这些损害导致了各种随机的改变而降低了信号的质量。对数字信号而言，则引起位串错误，比特 1 变为比特 0 或比特 0 变成比特 1。最有影响的传输损害包括衰减、延迟变形和噪声。

1．衰减

在任何传输介质上信号强度将随着距离延伸而减弱。对有线类传输介质，强度减弱或衰减一般具有对数函数性，对无线类传输介质，衰减则是距离和大气组成所构成的复合函数。

不可避免的衰减主要提出了三个问题。第一个问题就是接收到的信号必须有足够的强度，只有这样，接收器里的电子电路才能辨别、解释信号。第二个问题就是信号需比接收到的噪声维持一个更高的电平，以避免出错。第三个问题是针对模拟信号的，衰减是频率的增量函数，所以接收的信号会扭曲。

对于第一个和第二个问题可以用增加信号强度、设置放大器或中继器来解决。就点对点链路而言，发送器的信号强度必须足以为接收方所辨认，但是不能强到使发送器的电路过载，否则会产生变形信号。在超过一定距离后，信号衰减将会加大，这时使用放大器或中继器使信号再生。这些问题在多点线路里会变得复杂，这时从发送器到接收器的距离是可变的。

对于第三个问题可以使用技术手段使在某个频带内的频率衰减趋于相等。对于语音级电话线来说，通常使用在线路上加载线圈以改变线路的电气属性，结果使衰减效果趋于平滑。另一种方法是使用高频放大器将高频放大。

2．延迟变形

延迟变形是有线传输介质独有的现象，这种变形是由有线介质上信号传播速率随着频率而变化所引起的。在一个有限的信号频带中，中心频率附近的信号速度最高，而频带两边的信号速度较低，这样，信号的各种频率成分将在不同的时间到达接收器。

由于信号中各种成分延迟使得接收到的信号变形的这种效果称为延迟变形。延迟变形尤其对数字信号来说影响重大，一个位元的信号成分可能溢出到其他的位元，引起信号内部的相互串扰，这将限制传输控制上的位速率。

3．噪声

因传输系统造成的各种失真，以及在传输和接收之间的某处插入的不必要的信号产生了噪声。噪声可分为热噪声、内调制杂音、串扰、脉冲噪声 4 种。

热噪声是导体中电子的热振动引起的，它出现在所有电子设备和传输介质中，且是温度的函数。噪声值可以表示为 N=kTW。其中 k 为常数（1.3803×10–23J/°K)，T 为温度，W 为带宽。热噪声是在所有频谱中以相同的形态分布，所以常称为白噪声，它是不能够消除的，因此对通信系统性能就构成了上限。

当不同频率的信号共享同一传输介质时，可能导致内调制杂音。内调制杂音的结果往往产生一些新的信号，它们的频率是某两个频率和、差或倍数，这些信号可能对正常信号产生印象。当发送器、接收器或介入的传输设备里有一些非线性问题时，将会产生内调制杂音。

串扰是信号通路之间产生了不必要的耦合，这一般在邻近的双绞线之间因电耦合而产生，在极少数情况下也可能在运载多个信号的同轴电缆中产生。

脉冲噪声是非连续的且不可预测的。在短时间里，它可具有不规则的脉冲或噪声峰值，并且振幅较大。它产生的原因包括各种意外的电磁干扰，如闪电，以及通信系统的故障。脉冲噪声对模拟信号一般仅是小麻烦，但对数字信号是出错的主要原因。

1.2.2 数据通信系统

1.2.2.1 数据通信系统模型

数据通信系统的基本组成一般包括发送端、接收端以及收发两端之间的信道三个部分，如图 1-11 所示。

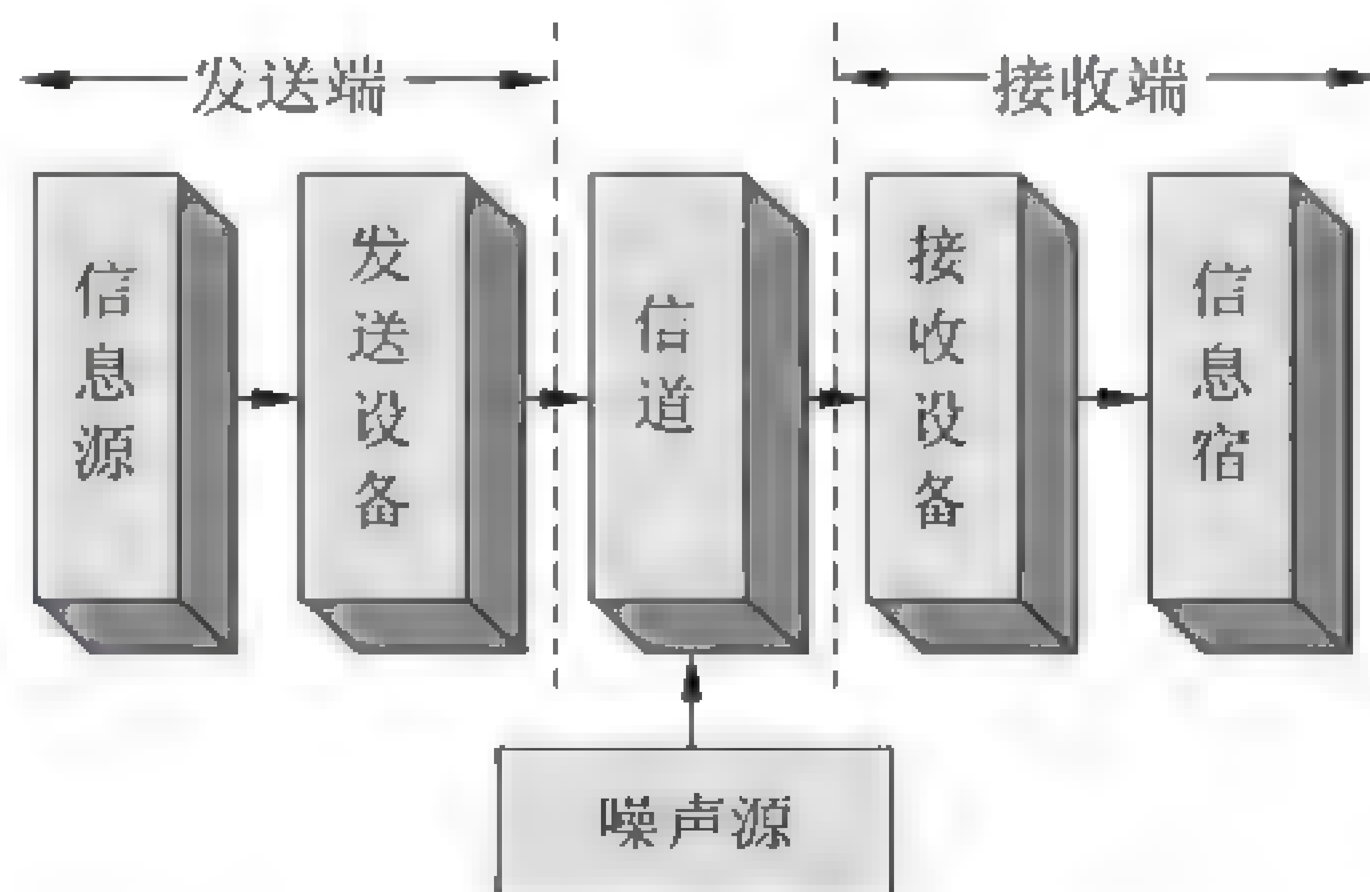


图 1-11 数据通信系统的模型

信息源是信息或信息序列的产生源，它泛指一切发信者，可以是人也可以是机器设备，能够产生诸如声音、数据、文字、图像、代码等电信号。信息源发出信息的形式可

以是连续的，也可以是离散的。

发送设备把信息源发出的信息变换成便于传输的形式，使之适应于信道传输特性的要求并送入信道的各种设备。发送设备是一个整体概念，可能包括许多的电路、器件与系统，比如把声音转换为电信号的麦克风，把基带信号转换成频带信号的调制器等。

信道是指传输信号的通道。根据传输媒质的不同，可分为有线信道（明线、电缆、光纤等）和无线信道（微波、卫星等）。明线和电缆可用来传输速率低的数字信号，其他信道均要进行调制。只经信道编码而不经调制就可直接送到明线或电缆中去传输的数字信号称为数字基带信号，经调制后的信号称为频带信号。信道噪声，可能是进入信道的各种外部噪声，也可能是通信系统中各种电路、器件或设备自身产生的内部噪声。

接收设备接收从信道传输过来的信息，并转换成信息宿便于接收的形式，其功能与发送设备的功能刚好相反。接收设备也是一个整体概念，可能包括许多的电路、器件与系统，比如把频带信号转换为基带信号的解调器，把数字信号转换为模拟信号的数/模转换器等。

信息宿是接收发送端信息的对象，它可以是人，也可以是机器设备。

按照信道中所传输信号的形式不同，通信系统可以进一步分为模拟通信系统和数字通信系统。数字通信系统的模型如图 1-12 所示，它完成信号的产生、变换、传递及接收。

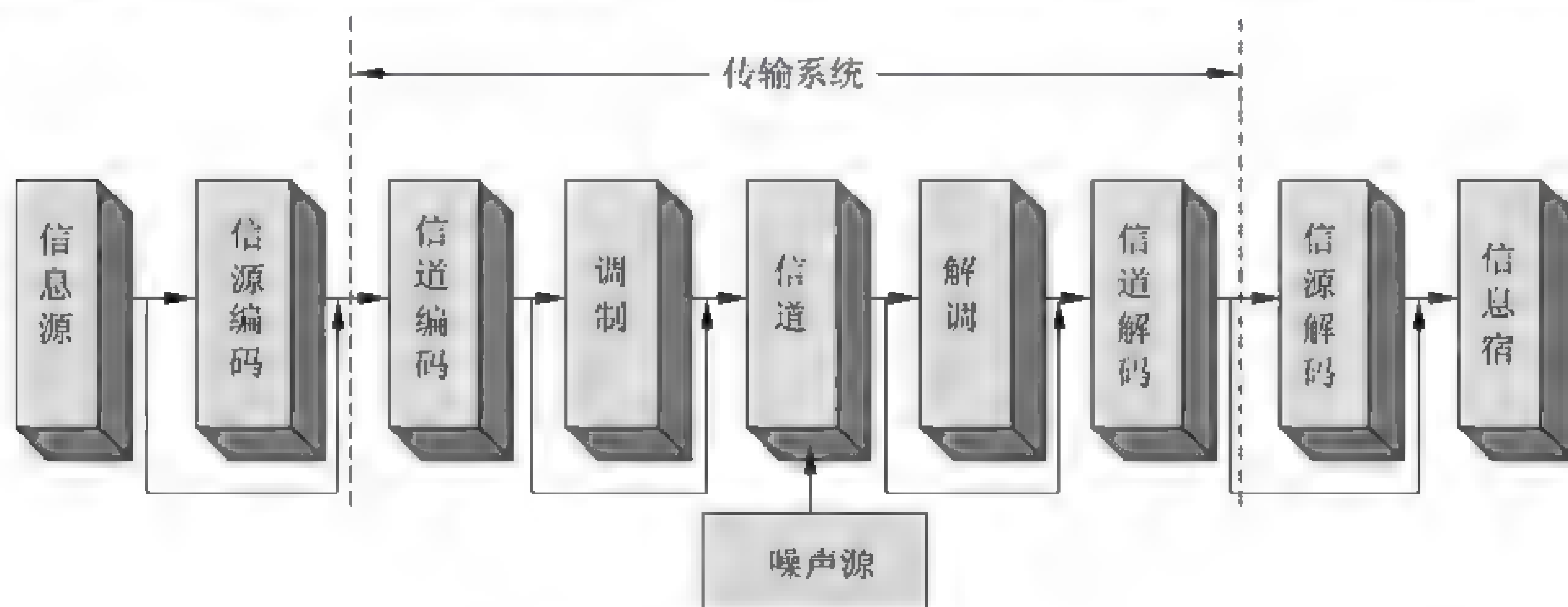


图 1-12　数字通信系统的模型

信源编码的主要功能是把人的话音以及机器产生的如文字、图表及图像等模拟信号变换成数字信号，即所谓的模/数（A/D）变换。在数字系统中，信源编码一般包括模拟信号的数字化和压缩编码两个范畴，压缩编码对数字信号进行处理，去除或减少信号的冗余度。

信道编码是将数字信号变换成与调制方式和传输信道匹配的形式，从而降低传输误码率，提高传输的可靠性。

根据信道媒质特性，对编码后的数字信号还要经调制后再送入信道中，如光纤信道

中的光调制，无线信道中的调频、调相、调幅等。

解调、信道解码和信源解码分别是调制、信道编码和信源解码的逆过程。

1.2.2.2 数据传输速率

为了提高数据的传输速率，我们总希望在一定时间内能够传输尽可能多的码元，然而任何实际的信道都不是理想的，在传输信号时会产生各种失真以及带来多种干扰。

即使信道比较理想，码元的传输速率也不是不受限制的。早在 1924 年，奈奎斯特（Nyquist）就推导出在理想低通信道下的最高码元传输速率的公式：

$$\text{理想低通信道的最高码元传输速率} = 2W$$

其中 W 是理想低通信道的带宽，单位为赫兹（Hz）。单位是 Baud（波特），1 波特为每秒传送 1 个码元。码元传输速率也称为调制速率。

该公式就是著名的奈氏准则。若码元的传输速率超过了奈氏准则所给出的数值，则将出现码元之间的相互干扰，以致在接收方无法正确判定在发送方所发送的码元是 1 还是 0。

由于码元的传输速率受奈氏准则的制约，所以要提高数据的传输速率，就必须设法使每个码元能携带更多个比特的信息量，这就需要采用多元制的调制方法。

1948 年，香农（Shannon）用信息论的理论推导出了带宽受限且有高斯白噪声干扰的信道的极限数据传输速率。当用此速率进行传输时，可以做到不产生误差。信道的极限数据传输速率 C 可表示为：

$$C=W\log_2(1+S/N)\ \text{bps}$$

其中 W 为信道的带宽，S 为信道内所传信号的平均功率，N 为信道内部的高斯噪声功率。

该公式亦称为香农公式，它表明，信道的带宽或信道中的信噪比越大，则信道的极限传输速率就越高。更重要的是，香农公式指出：只要数据传输速率低于信道的极限数据传输速率，就一定能找到某种办法来实现无差错的传输。

1.2.2.3 同步方式

在远距离传输数据时通常采用串行的方式，通信双方之间的数据信息沿着单根或几根通信线路传输，这时要考虑的问题之一就是同步。

1. 同步控制的方法

同步控制的方法包括异步起止方式和同步方式。

在异步起止方式中，接收方和发送方各自内部有时钟发生器，但频率必须一致。通信双方进行异步串行通信必须遵守异步串行通信控制规程，其特点是通信双方以字符作为数据传输单位，且发送方传送字符的间隔时间是不定的。

在同步串行通信方式中，以某种方式将发送方的时钟信号也发送过去，接收方用这个统一的时钟信号来选通数据信号，以此得到和发送完全一致的结果。由于同步串行通

信发送端和接收端具有统一的时钟信号，发送和接收的每一位信号都受同步信号的调整，因此，同步串行通信一次传送的信息量比异步串行通信大得多，但是付出的代价是设备复杂。

2．同步的实现

同步的实现包括位同步、字符同步、帧同步几个方面。

1）位同步

位同步是接收器从接收到的信号中正确地恢复原来数据信号的基础。实现位同步的方法有插入导频法和自同步法两种。插入导频法是在发送端发送的信号中插入专门的位同步导频信号，接收端把这个专门的导频信号检测出来作为位同步信号，如 FM 制编码、MFM 制编码等。自同步法是发送端不发送专门的位同步导频信号，只是控制连续 0 的个数不要太多，接收端设法从收到的数字信号中提取同步信息，如 HDB_3 编码。

2）字符同步

字符同步以字符为传输单位，其传输格式如图 1-13 所示。一个字符单位除表示信息的数据位外，还有若干个附加位：1 位起始位，恒为 0；可选的 1 位奇偶位；可选的停止位，可为 1 位、1.5 位或 2 位，恒为 1。传送一个字符，必须以起始位开始，以停止位结束。

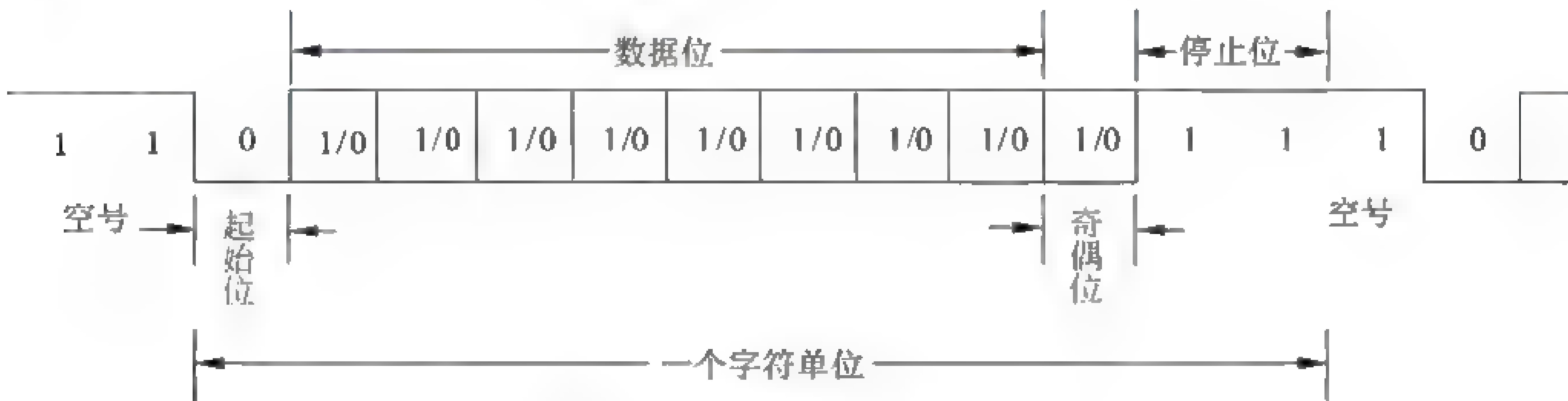


图 1-13　字符同步传输格式

3）帧同步

最初解决帧同步的方法是在帧之间插入时间间隔，依赖计时技术识别帧的开始和结束。但是，这种方法在网络上很难保证准确计时，所以又提出了其他方法。

（1）字符计数法。

字符计数法用一个特殊的字符表示一帧的开始，然后用一个字段标明该帧包含的字节数，当接收方收到该帧时，根据此字段提供的字节数，便可知道该帧的结束位和下一帧的开始位。

该种方法的主要问题是：如果计数字段在传输中出错，接收方就无法判断所传输帧的结束位，当然也无法知道下一帧的开始位，使发送方和接收方无法同步。即使接收方通过差错控制得知传输出错，也不知道应该让发送方跳回多少字符开始重传。

（2）带字符填充的首尾界符法。

带字符填充的首尾界符法在每一帧的头部用帧开始字符标记，在帧的尾部用帧结束字符标记。但是，在数据传输中，如果帧的首尾定界符出现在信息字段中，将会造成对数据的错误接收。为避免这种现象出现，采用在信息位中出现的定界符前填充转义字符的方法来区别。

（3）带位填充的首尾标志法。

带位填充的首尾标志法使用特定的位模式 01111110 作为帧的开始和结束标志。为了不使信息字段中出现的比特流 01111110 被误判为帧的首尾标志，发送方在信息位中每遇到 5 个连续的比特 1 时，将自动在其后插入一个比特 0，在接收方收到连续的 5 个比特 1 时，则自动删除后面紧跟的一个比特 0。

（4）物理编码违例法。

物理编码违例法将数据位“1”编码成高-低电平对，数据位“0”编码成低-高电平对。这样每一个数据位在中间都有一次跳变，使接收方容易将帧的边界定位。

1.2.3 数据调制与编码

虽然数字化已成为当今的趋势，但并不是使用数字数据和数字信号就一定是“先进的”，使用模拟数据和模拟信号就一定是“落后的”。数据究竟应当是数字的还是模拟的，是由所产生的数据的性质决定的。例如，运送话音信息的声波就是模拟数据，但数据必须转换成信号才能在网络媒体上传输。一般来说，模拟数据和数字数据都可以转换为模拟信号或数字信号。

1.2.3.1 数字数据编码为数字信号

对于数字数据，最普遍而且是最容易的编码方法就是用两个电压电平来表示两个二进制数字。例如，无电压表示数字 0，有电压表示数字 1，不归零制就是这种编码方式。

但是不归零制传输也有若干缺点。它难以决定一位的结束和另一位的开始，需要有某种方法使发送器和接收器进行定时。如果传输 1 或 0 过多，在单位时间内将有累积的直流分量。而且没有检错功能。为了克服上述缺点，编码方案有曼彻斯特编码和差分曼彻斯特编码、双极性半空占码（AMI）、双极性 8 零替换码（B8ZS）、三阶高密度双极性码（HDB_3）、nB/mB 码等。

1．曼彻斯特编码和差分曼彻斯特编码

曼彻斯特编码方法是将每一个码元再分成两个相等间隔，码元 1 是前一个间隔为高电平而后一个间隔为低电平，码元 0 则刚好相反。这种编码的好处就是可以保证在每一个码元的正中间时间出现一次电平的转换，利于接收方提取位同步信号，但是它所占的频带宽度比原始的基带信号增加了一倍。差分曼彻斯特编码规则是：若码元为 1 则其前

半个码元的电平与上一个码元的后半个码元的电平一样，若码元为 0 则其前半个码元的电平与上一个码元的后半个码元的电平相反。

2．双极性半空占码（AMI）

AMI 码编码规律如图 1-14 所示，原码序列中的“0”码仍为“0”，原码序列中的“1”码则交替变为+1 和 1。由于传号“1”码极性交替，如果接收端发现极性不是交替出现就一定出现了传输误码，因此可检出奇数个误码。但码流中连续 0 过多时，不利于定时提取。

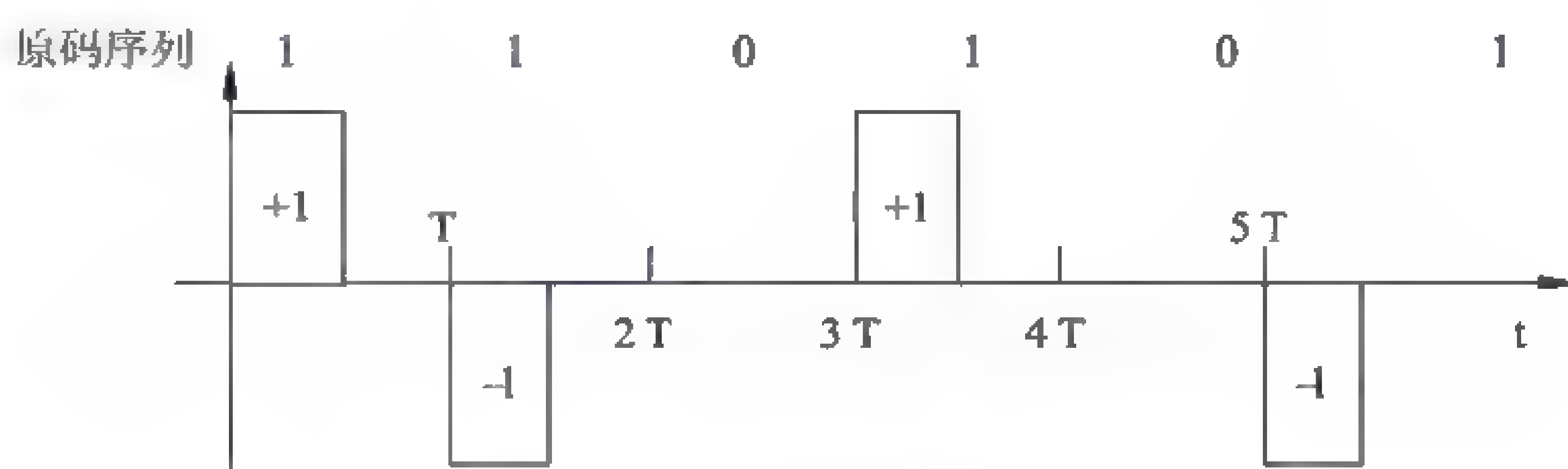


图 1-14　AMI 码的编码规律

3．双极性 8 零替换码（B8ZS）

B8ZS 为了克服 AMI 连零过多不利于定时提取的缺点，在 AMI 的基础上作了修改，其规则如下：

- 如果出现一个全零的 8 位组，并且在这个 8 位组之前的最后一个脉冲为正，那么这个 8 位组中 8 个 0 被编码为 $0001_{+}1_{-}01_{-}1_{+}$。
- 如果出现一个全零的 8 位组，并且在这个 8 位组之前的最后一个脉冲为负，那么这个 8 位组中 8 个 0 被编码为 $0001_{-}1_{+}01_{+}1_{-}$。

4．三阶高密度双极性码（HDB_3）

HDB_3 码保留了 AMI 码的所有优点，还可将连零限制在 3 个以内，克服了 AMI 码如果连零过多不利于定时提取的缺点。普通二进制码流变换为 HDB_3 码的规律如下：

① 在二进制码流中，当连续出现 4 个以上连“0”时，从第一个“0”起到 4 个连“0”中，最后一个“0”用“V”码取代，此码称为极性破坏点。

② 各“V”码必须进行极性交替。

③ 相邻“V”码间，前“V”码后邻的原传号码应与之符合极性交替原则。

④ 要使“V”码前邻一定出现一个与之极性相同的码位，按前二步变换后可能会出现与“V”码同极性的码，如果没有出现，就将四连“0”中的第一个“0”用“B”码取代，使“B”码与它后邻的“V”码同极性。

例：将二进制码流 100001011000000000011 进行 HDB_3 编码。

原码序列	1	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	1	1
①					V								V				V			
②					V_+								V_-				V_+			
③					V_+	1	0	1_+	1	0	0	0	V	0	0	0	V_+			
④	1_+	0	0	0	V_+	1_-	0	1_+	1_-	0	0	0	V_-	B_+	0	0	V_+	0	1_-	1_+

从上面的例子可以看出，当两个“V”码之间原传号码“1”为奇数个时，“V”码前邻必然会出现一个与之极性相同的码；当“1”码为偶数个时，第一个连“0”必然用 B 码取代。所以在接收端进行 HDB_3 解码时，在收到的码序列中检出相邻两个传号脉冲为同极性时，后者为“V”码。若相邻同极性码间连“0”数为 3，则第一个同极性码为原传号码，解码时只将“V”码变为“0”；若相邻同极性码间为两个连“0”时，则此两个连“0”前后原码均恢复为“0”。

5. nB/mB 码

nB/mB 码把 n 个二进制的码组转变为 m 个二进制的码组，$m>n$，因此实际的码组有 2^n 种，冗余码组有 2^m-2^n。

在高速光纤传输系统中，应用较为广泛的有 4B/5B、5B/6B、8B/10B、64B/66B。5B/6B 码是从 6 位二进制的 64 种组合中精选出 32 个码组对信源进行编码，其编码表如表 1-2 所示。该编码表列有正模式和负模式两种，使用时成对选择，以使得码序列中“1”和“0”的个数趋于平衡。5B/6B 码具有如下特性：

- 编码后的序列中最大的连 0 和连 1 个数为 5。
- 累积的 1，0 码个数的差值（称为数字和）在–3～+3 范围内变化，这一特性可用于误码监测。
- 各码组的数字和没有±1 的值，可用于码组同步。

表 1-2　5B/6B 编码表

输入二进制码组	输出二进制码组	
	正模式	负模式
00000	110010	110010
00001	110011	100001
00010	110110	100010
00011	100011	100011
00100	110101	100100
00101	100101	100101
00110	100110	100110
00111	100111	000111
01000	101011	101000
01001	101001	101001

续表

输入二进制码组	输出二进制码组	
	正模式	负模式
01010	101010	101010
01011	001011	001011
01100	101100	101100
01101	101101	000101
01110	101110	000110
01111	001110	001110
10000	110001	110001
10001	111001	010001
10010	111010	010010
10011	010011	010011
10100	110100	110100
10101	010101	010101
10110	010110	010110
10111	010111	010100
11000	111000	011000
11001	011001	011001
11010	011010	011010
11011	011011	001010
11100	011100	011100
11101	011101	001001
11110	011110	001100
11111	001101	001101

1.2.3.2　数字数据调制为模拟信号

模拟信号发送的基础就是载波信号，可用 $A\cos(\omega t+\phi)$ 表示，通过调制振幅、频率、相位三种载波特性之一或这些特性的某种组合来对数字数据进行编码。

1．基本的调制方法

最基本的调制方法有以下几种。

（1）幅移键控（Amplitude Shift Keying，ASK）：利用载波的振幅变化去携带数字数据，而载波的频率、相位都保持不变。

（2）频移键控（Frequency Shift Keying，FSK）：利用已调波的频率变化去携带数字数据，而载波的振幅、相位不变。

（3）相移键控（Phase Shift Keying，PSK）：利用已调波的相位变化去携带数字数据，而载波的频率和振幅都不变。

如图 1-15 所示的二进制幅移键控、频移键控和相移键控的例子。2ASK 中用载波有幅度和幅度为 0 分别表示数字数据的“1”和“0”；2FSK 中用两种不同的频率分别表示数字数据的“1”和“0”；2PSK 中用 0 相位和 π 相位分别表示数字数据的“1”和“0”。2ASK 信号带宽是 $2f_b$，f_b 是码元重复频率。2FSK 信号的抗噪性能优于 2ASK 信号，带宽为$\Delta f+2f_b$，Δf 为频差。2PSK 信号抗噪性能与 2ASK、2FSK 相比是最优的，带宽为 $2f_b$。

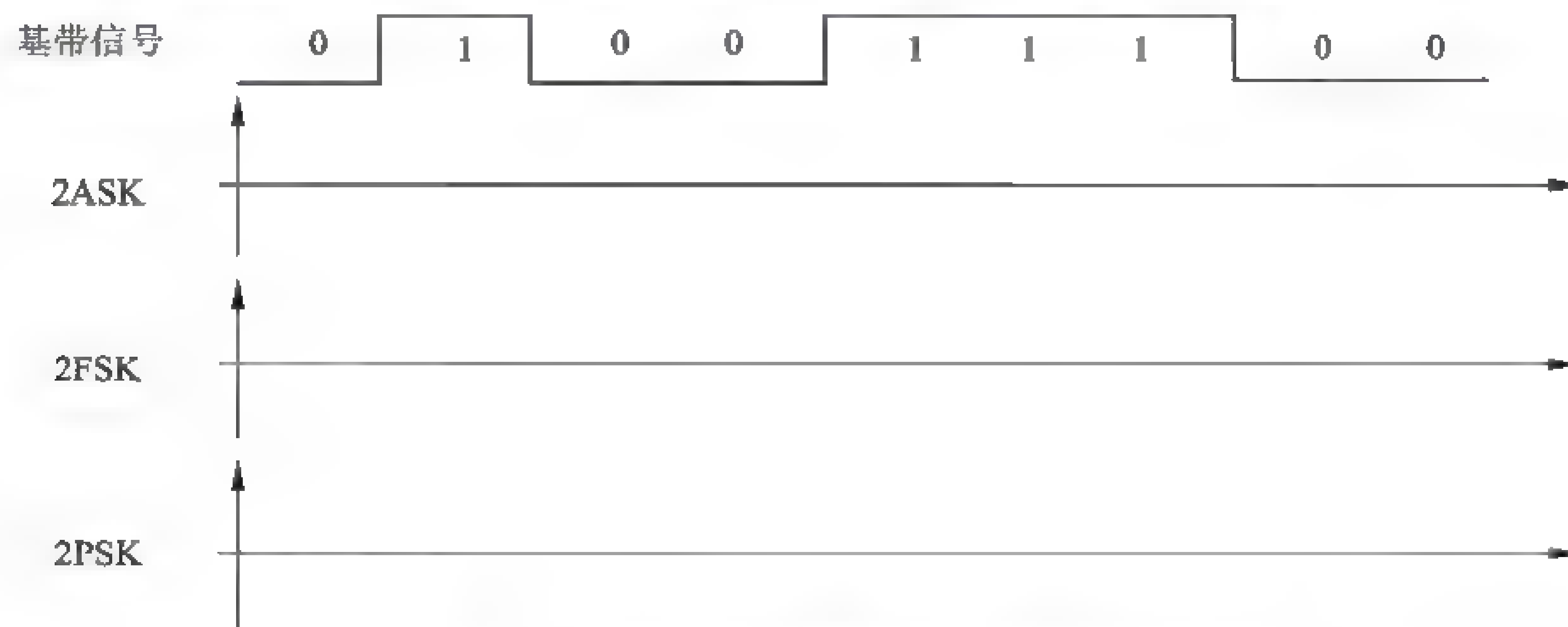


图 1-15 二进制幅移键控、频移键控和相移键控

在二相调制中，信号每变化一次，就发送一个比特的数据，为了提高数据的传输率，可以多个比特进行调制。一般而言，n 个比特位可以有 2^n 个组合，每个组合可以对应 2^n 不同模式中的一个，此时，比特率就是波特率的 n 倍，它们间的关系可用如下公式表示：

$$R_b=B\log_2 M$$

其中 R_b 为比特率，B 为波特率，M 为模式的数目。

2．正交振幅调制（Quadrature Amplitude Modulation，QAM）

信号模式的数目越多，意味着比特率相对于波特率的倍数越大，同时也将减小各种模式的信号之间的差别，接收方要将各种差别极小的幅度、频率和相位识别出来难度很大。一种普遍的解决方案就是结合使用振幅、频率和相位。正交振幅调制就是一种常用的技术，将幅移键控和相移键控结合在一起，把两个频率相同的模拟信号叠加在一起，一个对应正弦函数，一个对应余弦函数。M 进制的正交振幅调制可简记为 MQAM，其信号可表示为：

$$S(t)=C\sin(\omega t)+D\cos(\omega t)$$

MQAM 调制器与解调器的原理如图 1-16 和图 1-17 所示。在调制器中，二进制信号以比特率 f_B 送入调制器，经串/并变换后变成两路 $f_B/2$ 的二进制信号，再经过 2/L 变换器变成 L 进制和速率为 $f_B/2\log_2 L$ 的信号 A_i 和 B_i，接着进入两个相乘器，对两个相位差为 90°的正交载波进行调制，它们输出后即得 MAQM 信号。在接收端的解调器完成与调制器相反的功能。

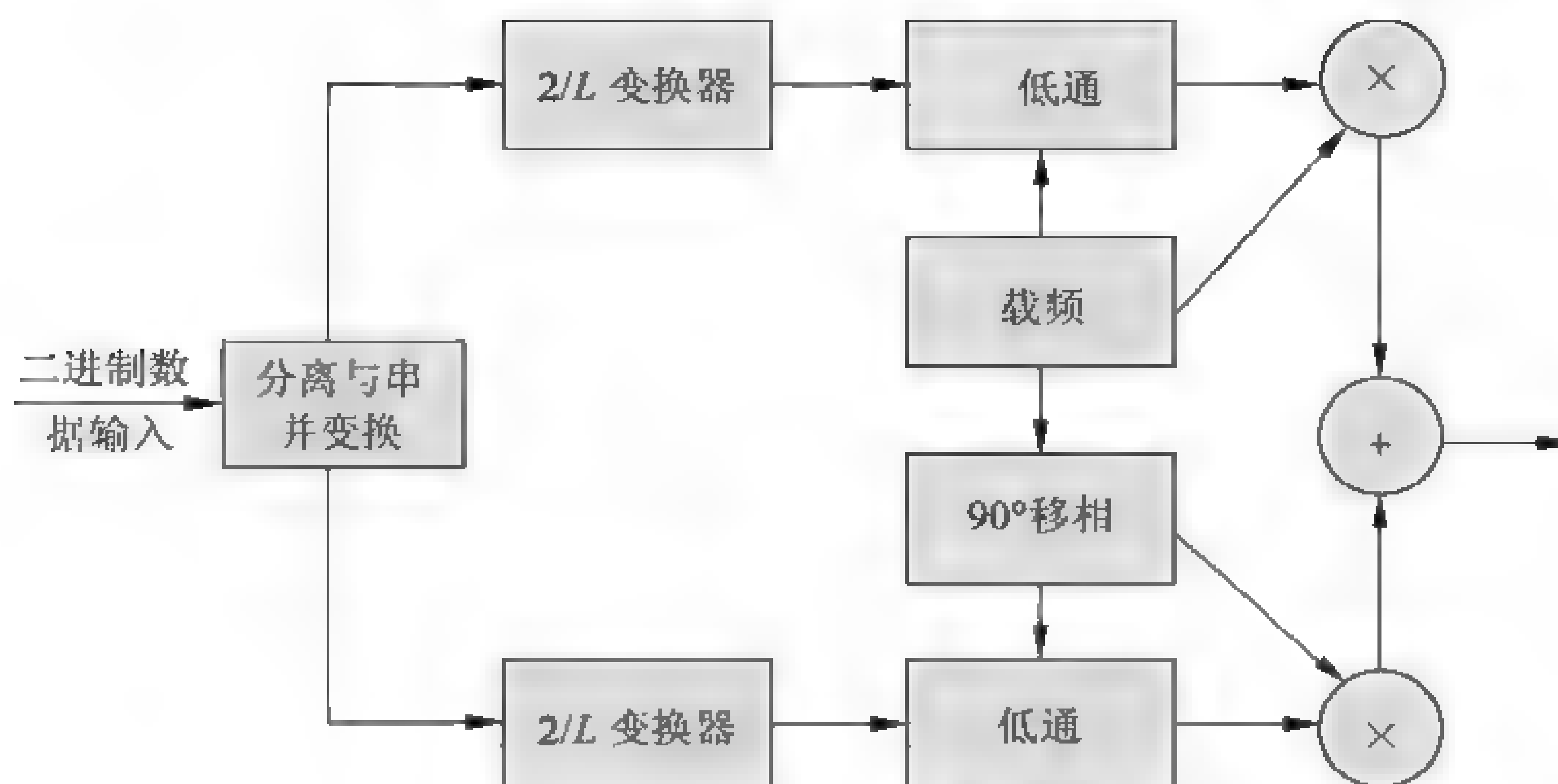


图 1-16　MAQM 调制器原理框图

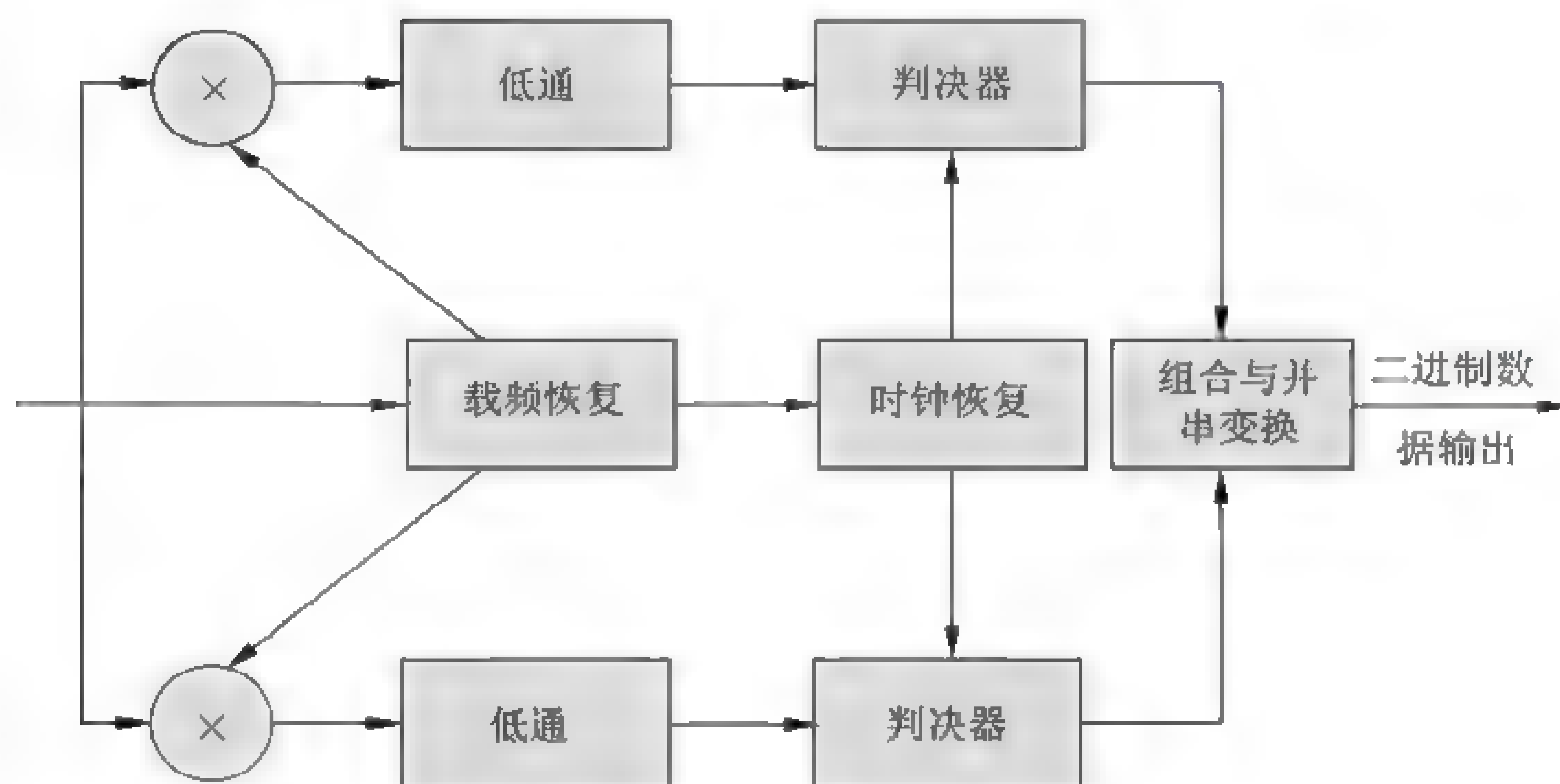


图 1-17　MQAM 解调器原理框图

1.2.3.3　模拟数据编码为数字信号

模拟数据编码为数字信号的第一步就是对模拟信号实施时域离散化。通常，信号时域离散化是用一个周期为 T 的脉冲信号控制采样电路对模拟信号 $f(t)$实施采样，得到样值序列 $f_s(t)$。如果取出的样值足够多，这个样值序列就能逼近原始的连续信号。但采样周期 T 取多大才能满足用样值序列 $f_s(t)$可代表模拟信号 $f(t)$的要求呢？采样定理可以解决这个问题。

低通采样定理：如果一个带限的模拟信号 $f(t)$的最高频率分量为 f_m，当满足采样频率 $f_s>2f_m$（$f_s=1/T$）时，所获得的样值序列 $f_s(t)$就可以完全代表原模拟信号 $f(t)$。

得到样值序列 $f_s(t)$后，就可以对每个样值进行编码了。编码的方法有很多，其中最

基本的就是线性的脉冲编码调制（Pulse Code Modulation，PCM）。线性的 PCM 由均匀量化和编码两部分组成。

量化是将样值幅度离散化的过程，也就是按某种规律将一个无穷集合的值压缩到一个有限集合中。所谓均匀量化是以等间隔对任意信号值来量化，即将信号样值幅度的变化范围[–*U*，+*U*]等分成 *N* 个量化级，记作Δ，则

$$\Delta=\frac{2U}{N}\qquad（U\text{称作信号过载点电压}）$$

根据量化的规则，样值幅度落在某一量化级区间内，则由该级的中心值一个值来量化。

获得量化值后，再用 *n* 位二进制码对其进行编码即可，码组的长度 *n* 与量化级数 *N* 之间的关系为：

$$N=2^n$$

例：一个模拟数据的电压变化范围为[–1V，1V]，采样值为 0.33V，采用线性 PCM 将其编码为 3 位二进制，解码后误差为多少？

首先求出 $N=2^3=8$，$\Delta=2\times1/8=0.25$。

然后设计出量化编码表，如表 1-3 所示。

表 1-3　量化编码表

变 化 区 间	量 化 值	编　码
[–1V，–0.75V)	–0.875V	000
[–0.75V，–0.5V)	–0.625V	001
[–0.5V，–0.25V)	–0.375V	010
[–0.25V，0V)	–0.125V	011
[0V，0.25V)	0.125V	100
[0.25V，0.5V)	0.375V	101
[0.5V，0.75V)	0.625V	110
[0.75V，1V]	0.875V	111

接着根据表 1-3 可知 0.33V 编码为 101。

最后接收方收到 101 后，也是根据表 1-3 解码为 0.375V，误差为 0.375V–0.33V=0.045V。

1.2.3.4　模拟数据调制为模拟信号

模拟数据经由模拟信号传输时不需进行变换，但是模拟数据本身的频率不高，由于考虑到天线发送时天线尺寸的问题，模拟形式的输入数据也需要在甚高频下进行调制，其输出信号是一种带有输入数据的频率极高的模拟信号。模拟数据调制为模拟信号有三种不同的调制技术：调幅（Amplitude Modulation，AM）、调频（Frequency Modulation，FM）与调相（Phase Modulation，PM），其中最常用的是调幅和调频。调频和调相调制

信号的频谱都是调制信号频谱的非线性变化，而且二者已调信号都反映出载波矢量角度上的变化，所以统称为角度调制。

1．调幅

调幅是一种使高频载波的幅度随着原始模拟数据的幅度变化而变化的技术。载波的幅度会在整个调制过程中变动，而载波的频率是不变的。调幅调制信号的表达式为：

$$s_{AM}(t)\ \ s(t)\cos\omega t$$

式中，$\cos\omega t$ 为载波，$s(t)$是要进行调制的基带信号。

2．调频

调频是一种使高频载波的频率随着原始模拟数据的幅度变化而变化的技术。因此，载波的频率在整个调制过程中波动，而载波的幅度是相同的。调频调制信号的表达式为：

$$s_{FM}(t) = A\cos[\omega t + \int_{-\infty}^{t} K_F m(t)\mathrm{d}t]$$

式中，K_F 代表调频器的灵敏度，$m(t)$为调制信号。

3．调相

调相是一种使高频载波的相位随着原始模拟数据的幅度变化而变化的技术。载波的相位在整个调制过程中变动，而载波的幅度是相同的。调相调制信号的表达式为：

$$s_{PM}(t) = A\cos[\omega t + K_P m(t)]$$

式中，K_P 代表调相器的灵敏度，$m(t)$为调制信号。

1.2.3.5　扩频通信

为了提高通信系统抗干扰性能，往往需要从调制和编码多方面入手，改进通信质量，扩频通信就是方法之一。由于扩频通信利用了扩展频谱技术，在接收端对干扰频谱能量加以扩散，对信号频谱能量压缩集中，因此在输出端就得到了信噪比的增益。

扩频通信是指系统占用的频带宽度远大于要传输的原始信号的带宽(或信息比特率)，且与原始信号带宽无关。通常规定：如果信息带宽为 B，扩频信号带宽为 f_{ss}，则扩频信号带宽与信息带宽之比 f_{ss}/B 称为扩频因子。

当 f_{ss}/B=1～2，即射频信号带宽略大于信息带宽时，称为窄带通信；

当 $f_{ss}/B \geq 50$，即射频信号带宽大于信息带宽时，称为宽带通信；

当 $f_{ss}/B > 100$，即射频信号带宽远大于信息带宽时，称为扩频通信。

扩频通信系统可以分为以下几种基本形式。

1．直接序列扩频（Direct Sequencing，DS）

直接序列扩频方式中，要传送的信息经伪随机序列编码后对载波进行调制。在发送端直接用扩频码序列去扩展信号的频谱，在接收端，用相同的扩频码序列进行解扩，将展宽的频谱扩展信号还原成原始信号，如图 1-18 和图 1-19 所示。因为伪随机序列的速率远大于要传送信息的速率，所以受调信号的频谱宽度将远大于要传送信息的频谱宽度。

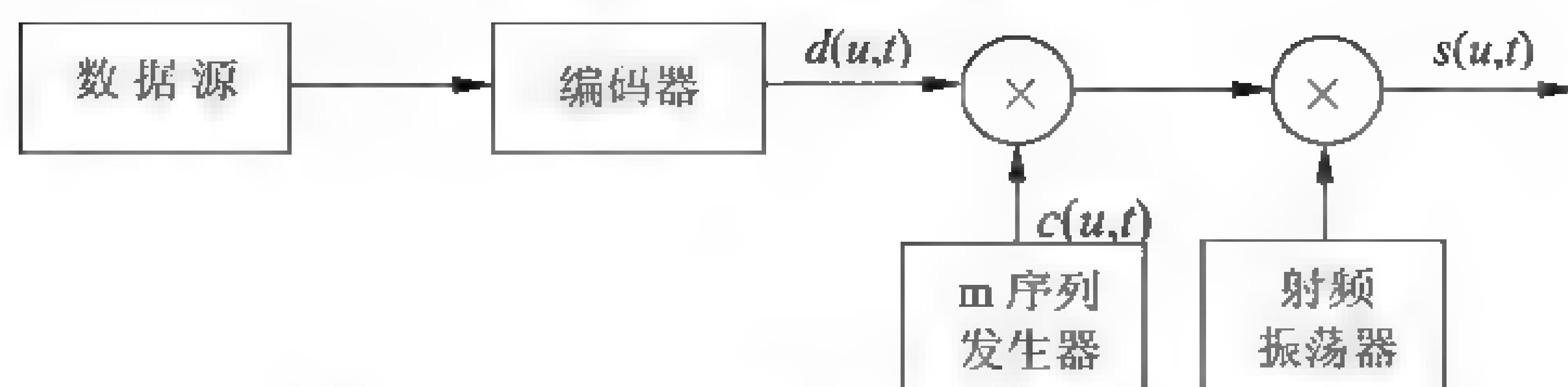


图 1-18 直接序列扩频系统的发送端原理图

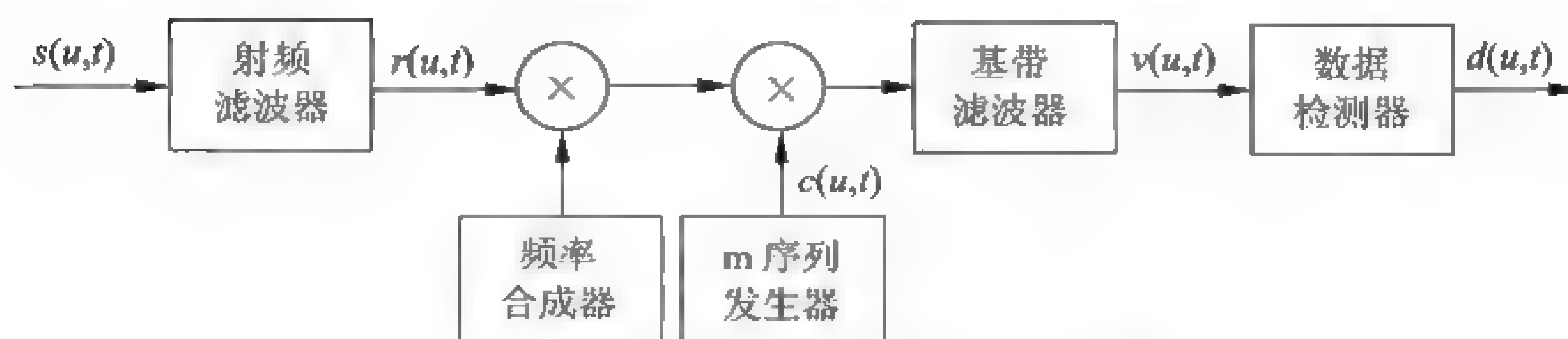


图 1-19 直接序列扩频系统的接收端原理图

2．跳频（Frequency Hopping，FH）

在跳频方式中，载波信息的信号频率受伪随机序列的控制，快速地在一个频段中跳变，此跳变的频段范围远大于要传送信息所占的频谱宽度，如图 1-20 所示。只要收、发信双方保证时-频域上的调频顺序一致，就能确保双方的可靠通信。在每一个跳频时间的瞬时，用户所占用的信道带宽是窄带频谱，随着时间的变换，一系列的瞬时窄带频谱在一个很宽的频带内跳变，形成一个很宽的调频带宽。

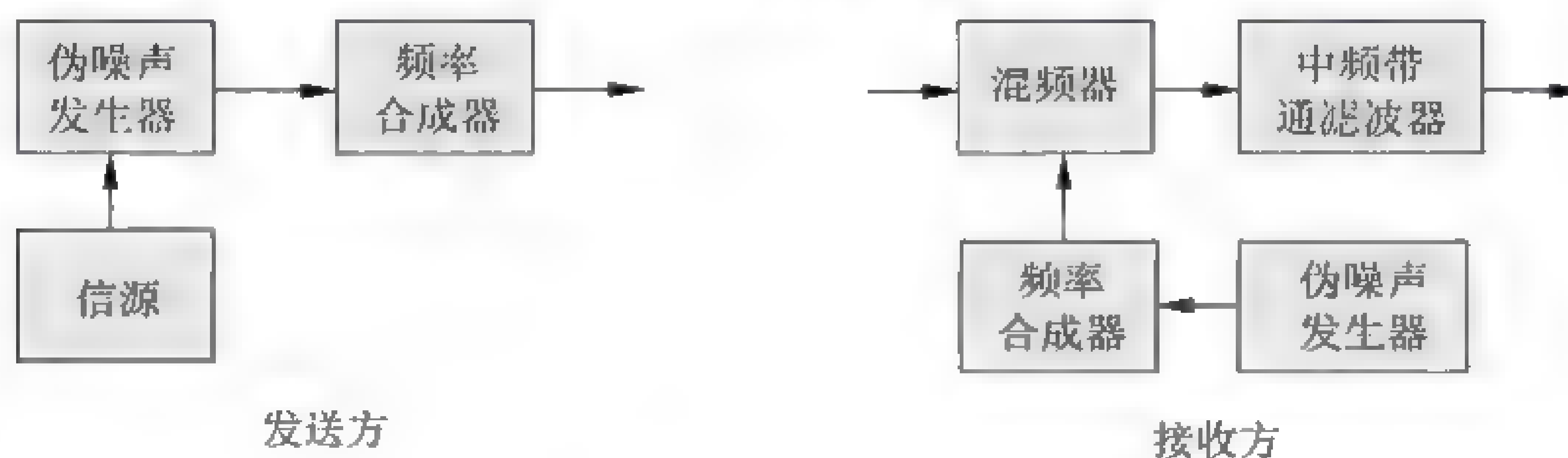


图 1-20 跳频系统原理图

3．跳时（Time Hopping，TH）

在跳时方式中，把每个信息码元划分成若干个时隙，此信息受伪随机序列的控制，以突发的方式随机地占用其中一个时隙进行传输。因为信号在时域中压缩其传输时间，相应地在频域中要扩展其频谱宽度。

4．线性调频扩频

线性调频扩频是指在给定脉冲持续间隔内，系统的载频线性地扫过一个很宽的频带。因为频率在较宽的频带内变化，所以信号的带宽被展宽。

1.2.4　多路复用技术

在点对点通信方式中，两点间的通信线路是专用的，其利用率很低，一种提高线路利用率的卓有成效的方法是使多个数据源合用一条传输线，这就是多路复用技术。多路复用系统将来自若干信息源的信息进行合并，然后将这一合成的信息群经单一的线路和传输设备进行传输，在接收方，则设有能将信息群分离成各个单独信息的设备。

多路复用的形式有时分多路复用、频分多路复用、波分多路复用等。

1.2.4.1　时分多路复用

时分多路复用（Time-Division Multiplexing，TDM）方法，其信号分割的参量是信号占用的时间，故要使复用的各路信号在时间上互不重叠，在传输时把时间分成小的时隙，每一时隙由复用的一个信号占用。如图 1-21 所示的情况，4 个用户 A，B，C 和 D 进行时分多路复用，4 个时隙构成一个时分复用帧，每一个时分复用的用户在每一个 TDM 帧中占用固定序号的时隙，每个用户所占用的时隙是周期性地出现。显然，时分复用的所有用户在不同的时间占用同样的频带带宽。

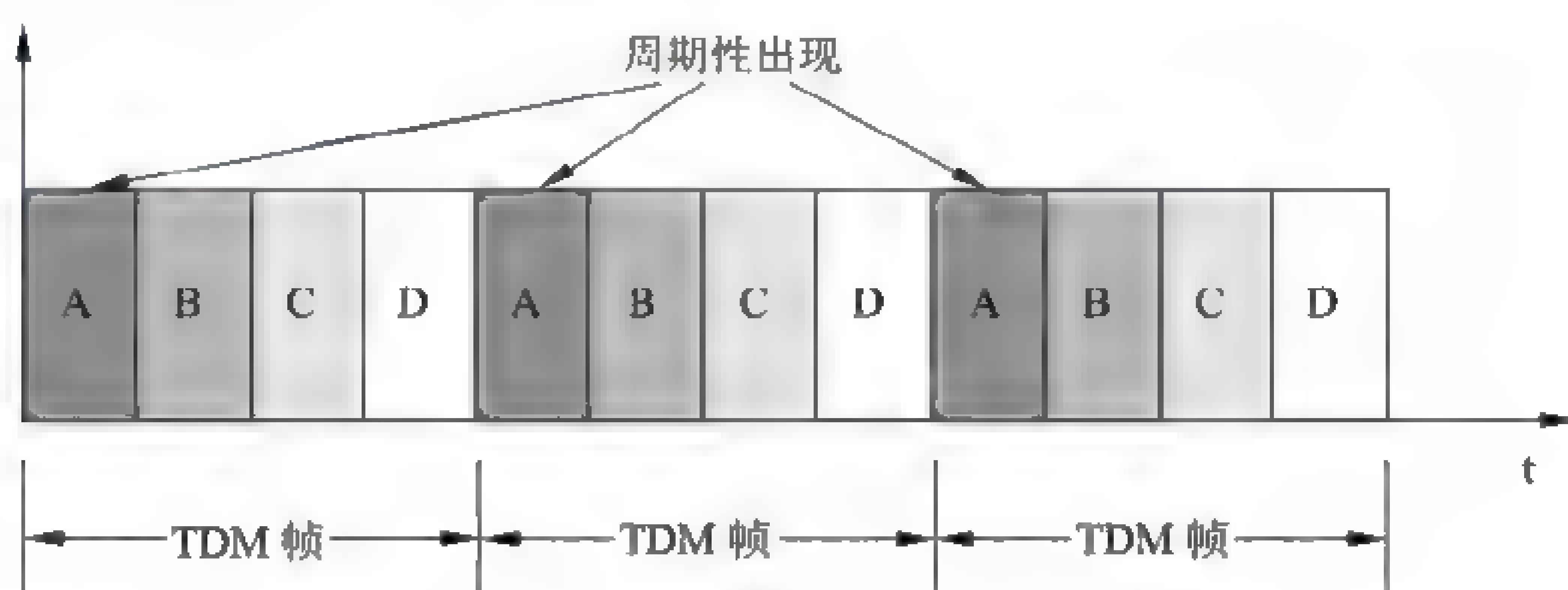


图 1-21　时分复用技术

在进行通信时，复用器和分用器总是成对地使用，在复用器和分用器之间是用户共享的高速信道。分用器的作用正好和复用器相反，它将高速线路传送过来的数据进行分组，分别送到相应的用户处。时分多路复用的通信模型如图 1-22 所示，为保证发送法和接收方两端正常通信，两端的旋转开关 S1 和 S2 的起始位置和旋转速度要完全相同。

当使用时分复用系统传送计算机数据时，由于计算机数据的突发性，一个用户对已经分配到的子信道的利用率一般不高，因为当用户在某一段时间暂时无数据传输时，那就只能让已经分配到的子信道空闲，而其他用户也无法使用这个暂时空闲的线路资源。

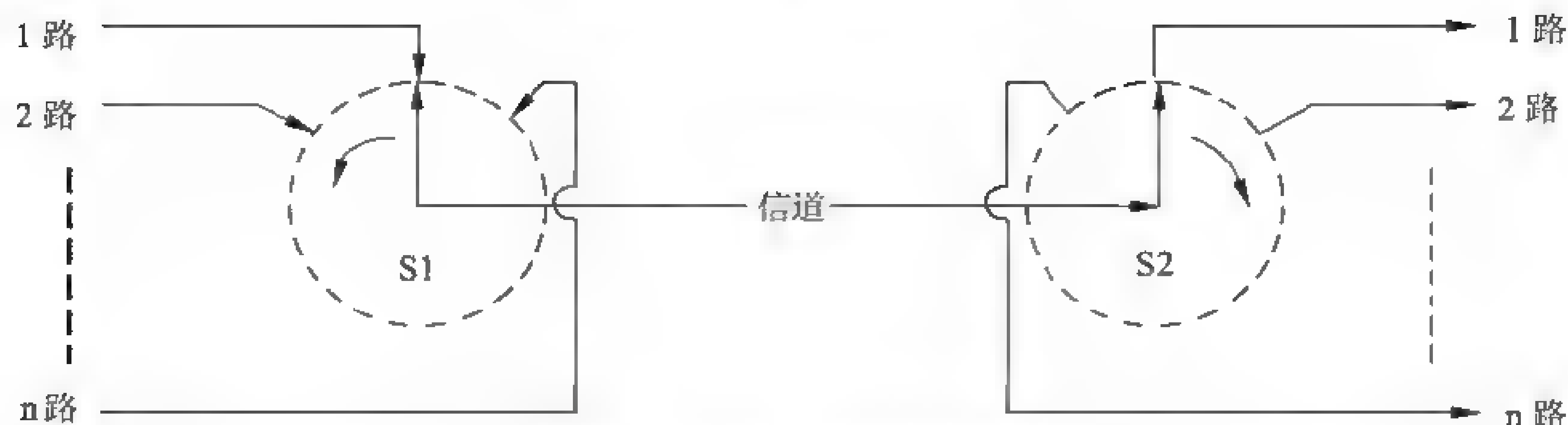


图 1-22 时分复用的通信模型

1.2.4.2 频分多路复用

频分多路复用（Frequency-Division Multiplexing，FDM）主要用于模拟信号。多路复用器接受来自多个源的模拟信号，每个信号有自己独立的带宽。接着这些信号被组合成另一个具有更大带宽更加复杂的信号，产生的信号通过某种媒体被传送到目的地，在那里另一个多路复用器完成分解工作，把各个信号单元分离出来。

频分多路复用的方法包含几个步骤。首先，传输媒体的可用带宽被划分成多个分离的信道，用户在分配到一定的频带后，在通信过程中自始至终都占用这个频带，如图 1-23 所示。然后，为每个信道定义一个载波信号，每一个载波信号形成了一个子信道，各条子信道的中心频率不相重合，子信道之间留有一定宽度的隔离频带。接着，利用载波信号对各个输入信号进行调制，从而产生调制信号。最后，所有调制信号被结合成一个更加复杂的单一模拟信号并传输出去。接收方借助于带通滤波器把各个独立的调制信号分离开来，并根据各个信道的频率选择恢复出原始信号。



图 1-23 频分复用技术

频分多路复用早已用在无带通滤波器及各种信道的频率选择无线电广播系统和有线电视系统（CATV）中。一根 CATV 电缆的带宽大约是 500MHz，可传送 80 个频道的电视节目，每个频道 6MHz 的带宽中又进一步划分为声音子通道、视频子通道以及彩色子通道。每个频道两边都留有一定的警戒频带，防止相互串扰。

1.2.4.3 波分多路复用

光纤技术的应用使得数据的传输速率空前提高，目前一根单模光纤的传输速率可达

到 2.5Gbps，如果设法对光纤传输中的色散问题加以解决，则一根光纤的传输速率可达到 10Gbps，但这几乎已到了单个光载波信号传输的极限值。使用一根光纤来同时传输多个频率很接近的光载波信号，又能使光纤的传输能力成倍地提高。由于光载波的频率很高，习惯上用波长而不是频率来表示所使用的光载波，所以波分多路复用（Wavelength-Division Multiplexing，WDM）就是光的频分复用。

在一根光纤上进行波分复用的方法很简单，如图 1-24 所示，两根光纤连到一个棱柱或衍射光栅上，每根的能力处于不同的波段，两束光通过棱柱或光栅合成到一根共享的光纤上，传送到远方的目的地后再分解开来。光纤系统使用的复用器即衍射光栅是完全无源的，因此极其可靠。

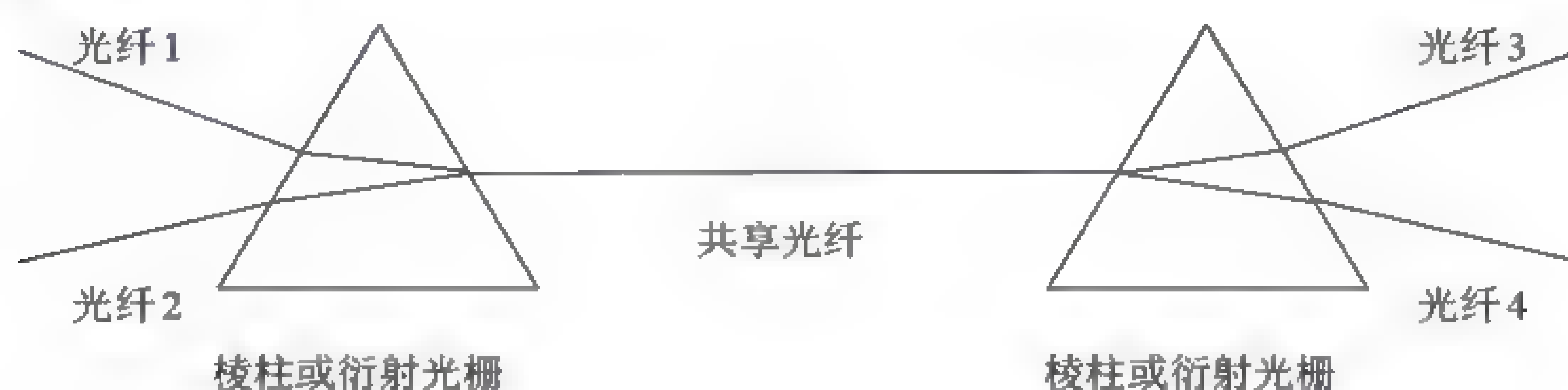


图 1-24　波分多路复用

波分复用系统主要由光发射机、光接收机、光放大器和光纤组成，如图 1-25 所示。在发送端，首先通过波长转换，将传输信号标准波长转换为波分复用系统使用的系列工作波长，然后多路光信号通过光合波器耦合到一根光纤上，经 BA 放大后在光纤上传输。传输一定距离后光信号会衰减，设置光纤中继器对光信号进行放大，为了对不同波长光信号具有相同的放大增益，采用掺铒光纤放大器（EDFA），而且 EDFA 不需要进行光电转换而直接对光信号进行放大。当光信号到达接收端后，将 PA 放大的光耦合信号解复用为多路光信号，然后通过波长转换，将每路的光信号的工作波长再转换为标准波长。

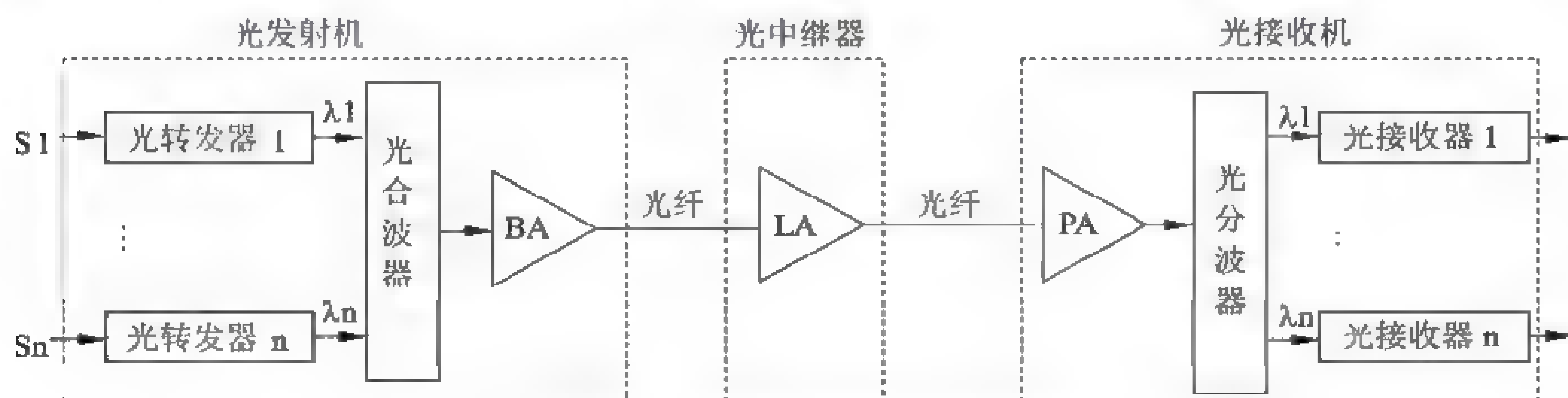


图 1-25　波分复用系统的组成

1.2.4.4　统计时分多路复用

统计时分多路复用（Statistic TDM，STDM）是一种改进的时分复用方法，它能明显

地提高信道的利用率。集中器常使用这种方法。

统计时分多路复用使用 STDM 帧来传送复用的数据，但每一个 STDM 帧中的时隙数小于或等于连接在集中器上的用户数，如图 1-26 所示，按 A，B，C，D 的顺序依次分配时隙。各用户有了数据就随时发往集中器的输入缓存，然后集中器按顺序依次扫描输入缓存，将缓存中的数据放入 STDM 帧中，对没有数据的缓存就跳过去。当一个帧的数据放满了，就发送出去。因此 STDM 帧不是固定分配时隙，而是按需动态地分配时隙。由于用户所占用的时隙并不是周期性地出现，所以在每个时隙中还必须有用户的地址信息，这是统计时分多路复用必须要有的和不可避免的开销。

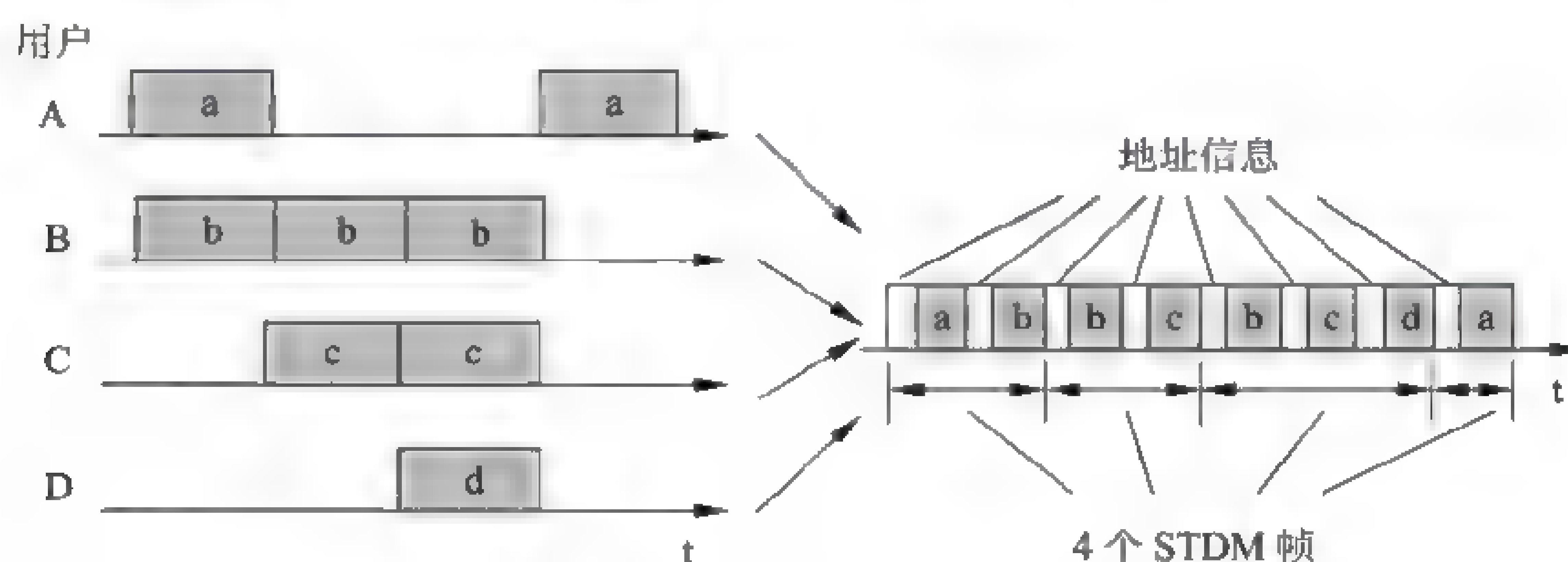


图 1-26 统计时分复用的工作原理

1.2.5 数据交换方式

1.2.5.1 线路交换

两个终端开始正式通信之前，首先由主呼终端进行呼叫，送出被呼终端的电话号码，直到在主呼和被呼之间建立起一条专用的通信线路，主呼终端和被呼终端才开始进行双向数据传输，在整个数据传输期间一直独占线路，通信结束后释放已建立的通信线路，这种技术叫做线路交换（circuit switching），主要用于电话系统。所谓“交换”体现在交换设备内部。当交换机从一条输入线接收到呼叫请求时，首先根据被呼叫者的号码寻找一条合适的空闲输出线，然后通过硬件开关将二者连通。从通信资源的分配角度来看，“交换”就是按照某种方式动态地分配传输线路的资源。

线路交换技术有两大优点。第一个是传输延迟小，唯一的延迟是电磁信号的传播时间；第二个是一旦线路接通，便不会产生冲突，因为通信双方独享物理线路。

线路交换技术也有两个缺点。第一个是建立线路所需的时间很长，在数据传输开始前，呼叫信号必须经过若干个中间交换机。另一个是由于线路独享造成资源浪费，因为线路一旦被建立起来，即便空闲也不能被其他用户所用。

1.2.5.2　报文交换

发送方待发送的整个数据块称为报文（message）。报文交换事先不建立线路，当发送方有数据块要发送时，它把目的地址附加在报文上交给交换设备，交换设备选择一条合适的空闲输出线，将报文通过该输出线传送出去。在这个过程中，交换设备的输入线和输出线之间不建立物理连接，在每个交换设备处，报文首先被存储起来，在适当的时候被转发出去，所以报文交换采用的是存储转发技术，动态分配线路，使得线路能够共享，提高了资源的利用率。

但是，报文交换对传输数据块的大小没有限制，当传输大报文时，交换设备必须利用大容量磁盘进行缓存，而且可能占用一个交换设备到另一个交换设备的线路长达几分钟，因此报文交换不适合交互式通信。

1.2.5.3　分组交换

为了解决报文交换大报文传输的问题，分组交换技术严格限制数据块大小的上限，把大报文切分成更小的数据单位，加上一些必要的控制信息组成的首部后，就构成了分组（packet），使分组可以在交换设备的内存中缓存，同时保证任何用户都不能独占线路超过几十毫秒。

现代网络绝大多数采用分组交换技术。分组交换网由若干个交换机和连接这些交换机的链路组成，每台主机都有一条到交换机的链路，交换机的主要工作就是在它的一条链路上接收输入分组，把这些分组从其他的链路上输出。

根据内部机制的不同，分组交换技术又分为数据报（datagram）和虚电路（virtual circuit）两种方式。

1．数据报

在数据报方式中，每个分组的首部都带有完整的目的地址，交换机根据转发表转发分组。

如图 1-27 所示的例子，假定主机 A 和主机 B 分别要向主机 E 和主机 F 发送分组。主机 A 先将分组逐个地发往与它直接相连的交换机 1，交换机 1 将主机 A 发来的分组缓存，然后查找自己的转发表，不同时刻转发表的内容可能不相同，因此有的分组转发给交换机 2，有的分组转发给交换机 3。当分组正在链路交换机 1-交换机 2 和链路交换机 1-交换机 3 上传送时，分组并不占有网络其他部分的资源。接着交换机 2 和交换机 3 将分组转发给交换机 5，最后交换机 5 将分组直接转发给主机 E。因为采用存储-转发技术，资源是共享的，所以主机 A 在发送分组时，主机 B 也可同时发送分组给 F。

通过上面的例子，可以看出数据报方式具有如下特点：

（1）在具有多个分组的报文中，交换机尚未接收完第二个分组，已经收到的第一个分组就可以转发出去，不仅减小了延迟，而且提高了吞吐量。

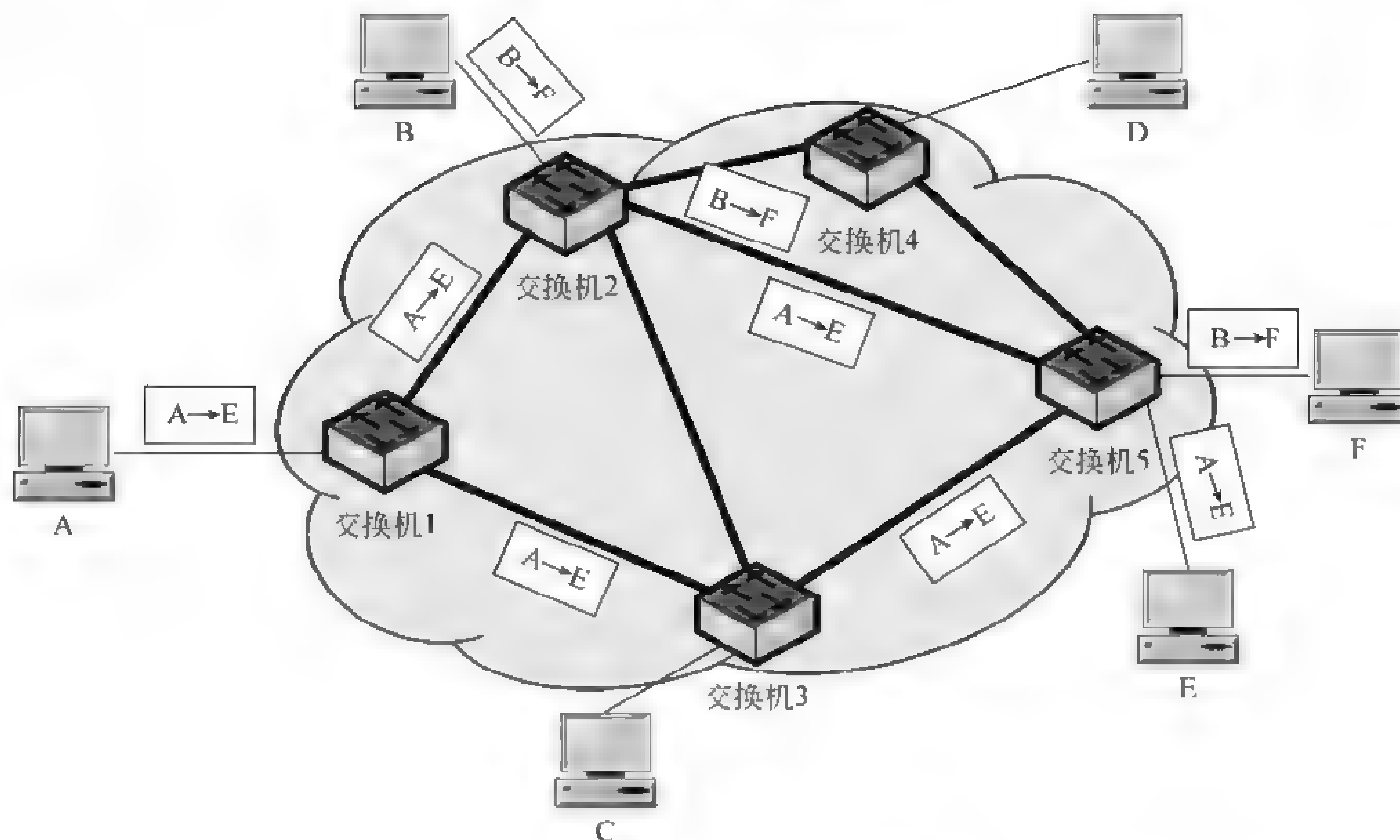


图 1-27 数据报方式转发分组

（2）资源利用率高。

（3）发送分组前不需要建立连接。

（4）具有冗余路径，当一台交换机或一段链路故障时，可相应地更新转发表，寻找到另一条替代路径转发分组，对故障适应力强。

（5）每个分组都独立处理，转发的路径可能不同，因此不一定按序到达接收方。

（6）分组在各交换机进行存储转发时需要排队，这会造成一定的时延。

2．虚电路

虚电路方式要求在发送数据之前，在源主机和目的主机之间建立一条虚连接。在建立连接阶段，需要在源主机和目的主机之间的每一个交换机上建立“连接状态”，连接状态由连接经过的每个交换机中的“VC 表”记录组成。在一个交换机上的 VC 表中一条记录包括：

- 虚电路标识符（Virtual Circuit Identifier，VCI），在这个交换机上唯一标识连接，并且将放在属于这个连接的分组首部内传送。
- 由这个 VC 到达交换机的分组的输入接口。
- 从这个 VC 离开交换机的分组的输出接口。
- 用于输出分组的一个不能不同的 VCI。

在建立一个新连接时，要在连接所要经过的每段链路上分配一个 VCI 值，并确保在一段链路上选定的 VCI 值未被该链路上已经存在的某个连接使用。连接状态的建立有两类方法。一类是由网络管理员配置连接状态，这样的虚电路是永久虚电路（Permanent

Virtual Circuit，PVC），它最好被看作长期生存的或可管理配置的 VC，当然，管理员也可以删除 PVC。另一类是主机发送消息给网络建立连接状态，这样建立的虚电路称为交换虚电路（switched virtual circuit），它可由主机动态的建立和删除。

如图 1-28 所示的一个例子，链路上的数字代表接口号，分组首部的数字为 VCI。现在主机 A 要向主机 B 发送数据，在建立连接阶段，假设三个交换机的 VC 表增加的记录如表 1-4 所示。

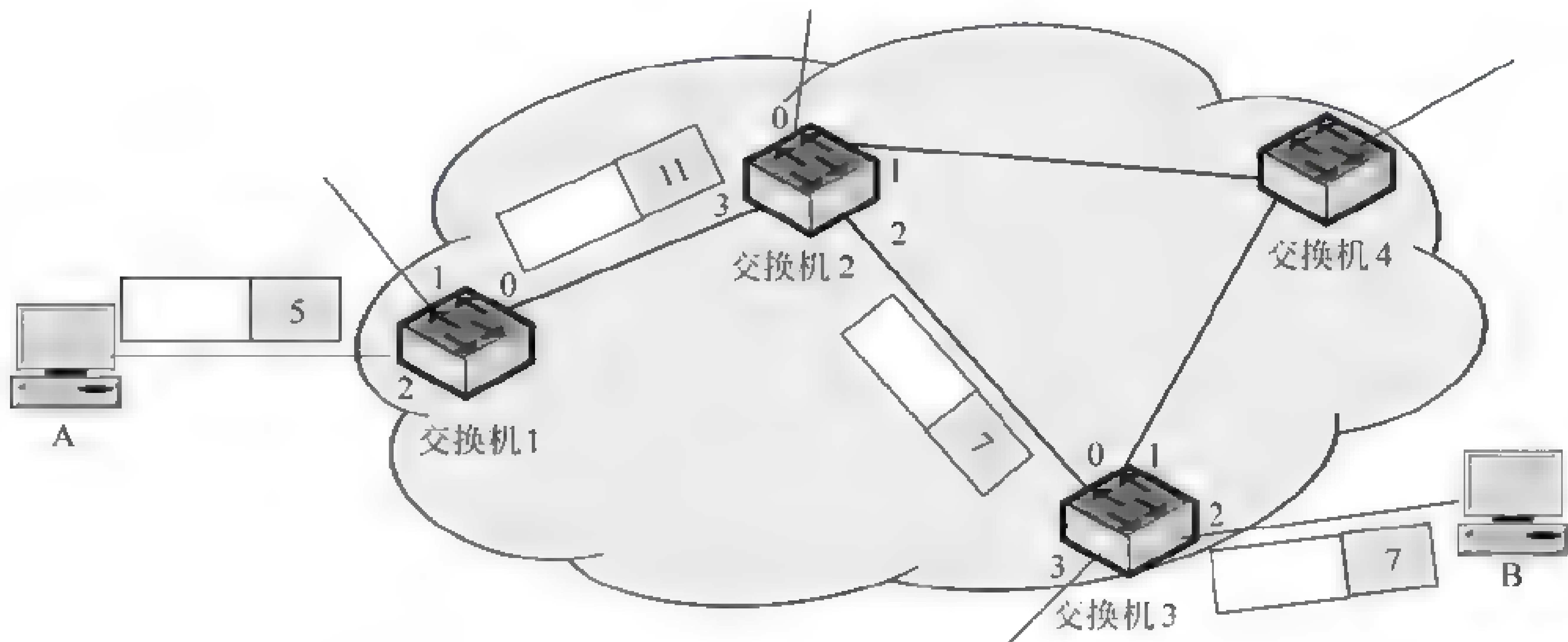


图 1-28　虚电路方式转发分组

表 1-4　VC 表增加的记录

交换机 1	输入接口	输入 VCI	输出接口	输出 VCI
	2	5	0	11
交换机 2	输入接口	输入 VCI	输出接口	输出 VCI
	3	11	2	7
交换机 3	输入接口	输入 VCI	输出接口	输出 VCI
	0	7	2	7

一旦 VC 表被建立，就可以进入数据传输阶段。对于每一个要发往主机 B 的分组，主机 A 将值为 5 的 VCI 放入分组首部并发送给交换机 1。如果分组在指定的输入接口到达并且首部包含指定的 VCI 值，那么交换机先将这个分组的首部 VCI 替换成指定的输出 VCI 并将分组发送到指定的输出端口。交换机 1 在接口 2 上接收到 VCI 为 5 的分组后，查询 VC 表，接着将 VCI 修改为 11，最后从接口 0 输出，这样分组从接口 3 到达了交换机 2。此过程继续，直到分组携带 VCI 为 7 到达主机 B，主机 B 由此识别这个分组来自主机 A。

通过上面的例子，可以看出数据报方式具有如下特点：

（1）用户间通信必须建立连接，数据传输过程中再不需寻找路径，相对数据报方式时延相对较小。

（2）通常分组走同样的路径，所以按序到达接收方。

（3）资源利用率高。

（4）分组首部并不包含目的地址而是 VCI，相对数据报方式开销较小。

（5）如果一个连接上有交换机或链路出现故障，连接就会破坏，必须建立一个新的连接，同时需要撤销原来的连接，释放交换机中虚电路表的存储空间。

（6）在发送第一个分组前有一定的延迟。

1.2.5.4 信元交换

信元交换是异步传输模式（Asynchronous Transfer Mode，ATM）采用的交换方式，在很大程度上就是按照虚电路方式进行分组转发。在 ATM 网络中与众不同的一点是，分组长度是固定不变的，称为信元（cell）。信元长度为 53 字节，5 字节的首部，48 字节的有效载荷，其结构如图 1-29 所示。ATM 信元有两种不同的首部，分别对应于用户到网络接口（User-to-Network Interface，UNI）和网络到网络接口（Network-to-Network Interface，NNI）。

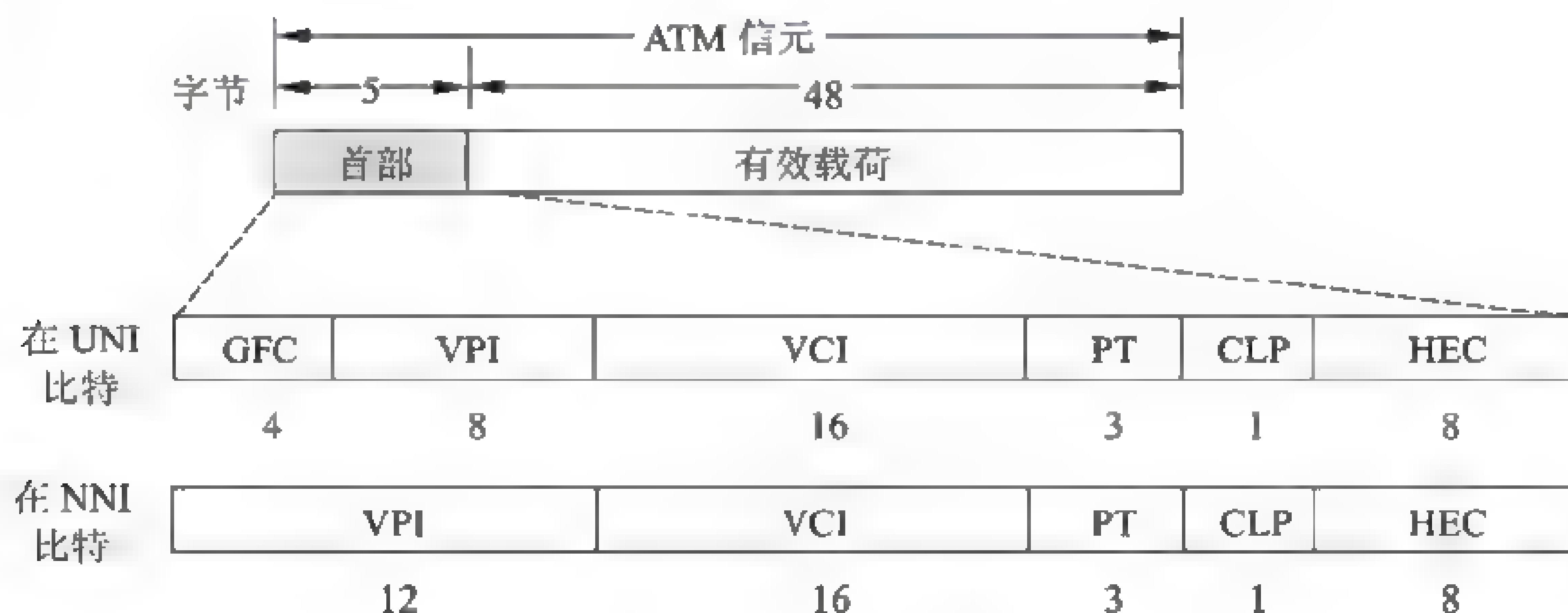


图 1-29 ATM 信元结构

ATM 信元首部中各字段的作用如下：

（1）通用流量控制（Generic Flow Control，GFC）。GFC 用来在共享媒体上进行接入流量控制，现在未用，通常置为 0。

（2）虚通道标识符 VPI/虚通路标识符 VCI。一个虚通路（Virtual Channel，VC）是在两个或两个以上的端点之间的一个传送 ATM 信元的通信通路，一个虚通道（Virtual Path，VP）包含有许多相同端点的虚通路，而这许多复用在一条链路上的虚通路都使用同一个虚通道标识符（Virtual Path Identifier，VPI），复用在一个 VP 中的不同虚通路用它们的虚通路标识符（Virtual Channel Identifier，VCI）来识别。图 1-30 表示了使用 VPI

和 VCI 标识 VP 和 VC 的方法。

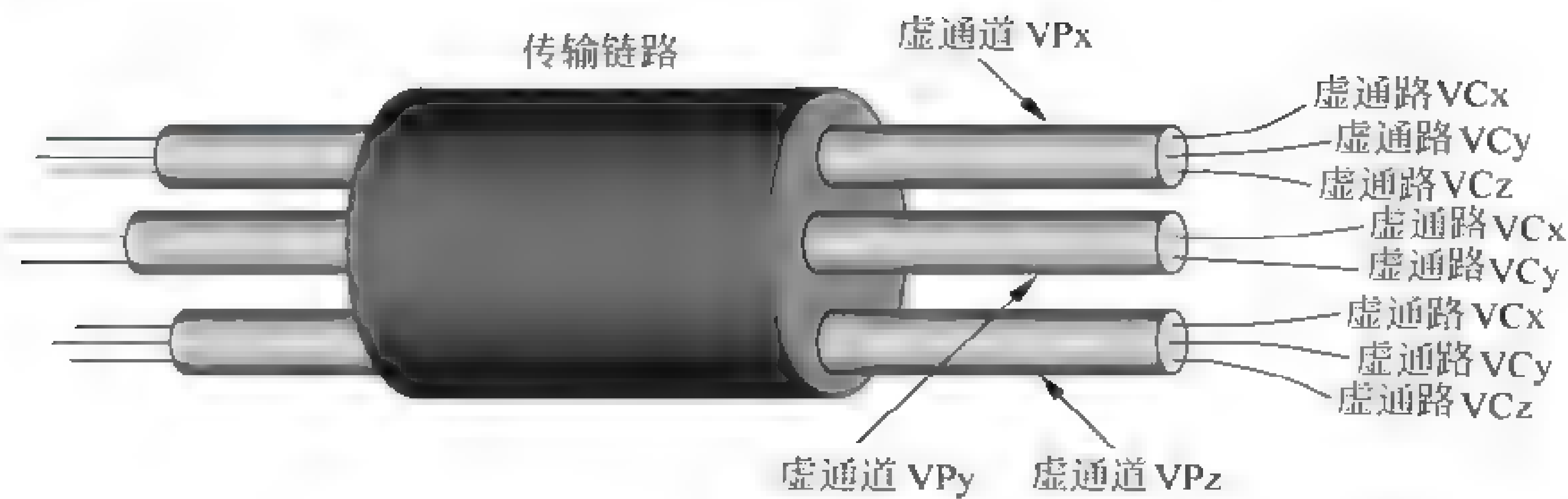


图 1-30　ATM 连接的标识符 VCI 和 VPI

（3）有效载荷类型（Payload Type，PT）。PT 用来区分该信元是用户信息还是非用户信息。

（4）信元丢失优先级（Cell Loss Priority，CLP）。CLP 指示信元的丢失优先级，当网络负荷很重时，ATM 交换机首先丢弃 CLP=1 的信元以缓解网络可能出现的拥塞。

（5）首部差错控制（Header Error Control，HEC）。HEC 只对首部的前 4 个字节进行循环冗余校验。

1.2.5.5　广播

所谓广播，指同时向网上所有主机发送报文，是一种特殊的交换方式。许多物理网络本身便是广播型的，广播型的网络用一个传输介质将所有主机连接起来，比如总线型网络和以微波、卫星方式传播的网络。也有许多网络是点到点型的，这种网络的广播必须由软件实现，比如采用扩散的方式，把收到的分组，从除了分组到来的端口外的所有输出端口上发出。

1.2.6　传输介质

传输介质是数据传输系统中在发送设备和接收设备之间的物理通路，也称为传输媒体，可分为导向传输介质和非导向传输介质两类。在导向传输介质中，电磁波或光波被导向沿着固体媒体传播，其包括双绞线、同轴电缆、光纤等，而非导向传输介质就是指自由空间，其传输方式包括微波、无线电、红外线等。

1.2.6.1　双绞线

把两根互相绝缘的铜导线并排放在一起，然后用规则的方法绞合起来就构成了双绞线。绞合可减少对相邻导线的电磁干扰。为了提高双绞线的抗电磁干扰的能力，可以在双绞线的外面再加上一个用金属丝编织成的屏蔽层，这就是屏蔽双绞线（Shielded Twisted

Pair，STP），无屏蔽层的双绞线就称为非屏蔽双绞线（Unshielded Twisted Pair，UTP），它们的结构如图 1-31 所示。



图 1-31 双绞线的结构

1991 年，美国电子工业协会 EIA 和电信工业协议 TIA 联合发布了一个标准 EIA/TIA-568，这个标准规定用于室内传送数据的非屏蔽双绞线和屏蔽双绞线的标准。随着局域网上数据传送速率的不断提高，EIA/TIA 在 1995 年将布线标准更新为 EIA/TIA-568-A，此标准规定了从 1 类线到 5 类线的 5 个种类的 UTP 标准，其中 3 类线和 5 类线用于计算机网络。3 类线由两条轻轻拧在一起的线构成，一般在塑料外壳内有 4 对这样的线，如图 1-32 所示。5 类线和 3 类线相似，但拧得更密，并以特富龙材料绝缘，交互感应少，更适用于高速计算机通信。



图 1-32 4 对线的非屏蔽双绞线

模拟传输和数字传输都可以使用双绞线，其通信距离一般为几到十几公里。距离太长时，对于模拟传输要加放大器以便将衰减的信号放大到合适的数值，对于数字传输则要加中继器以便将失真的数字信号进行整形。由于双绞线的价格便宜且性能也不错，使用十分广泛。

1.2.6.2　同轴电缆

同轴电缆由内导体铜质芯线、绝缘层、网状编织的外导体屏蔽层以及保护塑料外层所组成，如图 1-33 所示。由于外导体屏蔽层的作用，同轴电缆具有很好的抗干扰特性，广泛用于传输较高速率的数据。

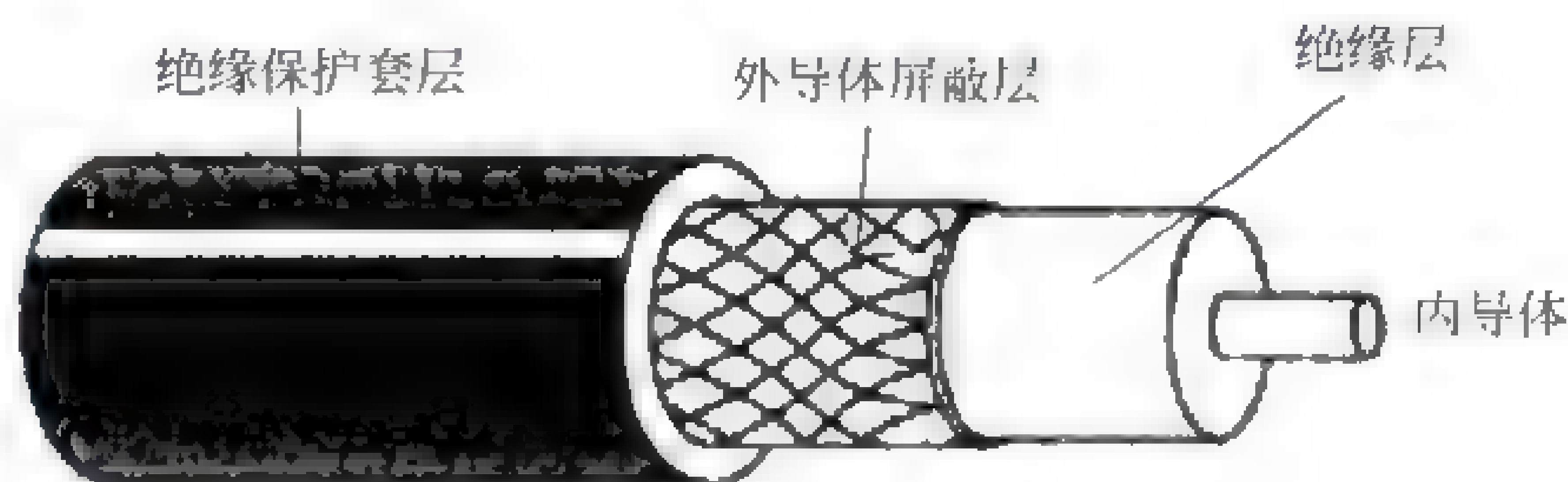


图 1-33　同轴电缆的结构

当需要将计算机连接到同轴电缆上的某处时，比用双绞线要麻烦得多，通常使用 T 型分接头。T 型分接头主要有两种，一种必须先把电缆剪断，然后进行连接；另一种则不必剪断电缆，使用较昂贵的、特制的插入式分接头，利用螺丝分别将两根电缆的内外导线连接好。

通常按特性阻抗数值的不同，将同轴电缆分为两类。

1．50Ω同轴电缆

50Ω同轴电缆主要用于在数据通信中传送基带数字信号，又称为基带同轴电缆，在局域网中得到广泛应用。用这种同轴电缆以 10Mbps 的速率可将基带信号传送 1km。

在传输基带数字信号时，可以使用曼彻斯特编码和差分曼彻斯特编码解决同步问题。

2．75Ω同轴电缆

75Ω同轴电缆主要用于模拟传输系统，是有线电视系统（CATV）中的标准传输电缆。在这种电缆上传送的信号采用了频分复用的宽带信号，因此 75Ω同轴电缆又称为宽带同轴电缆。宽带同轴电缆用于传输模拟信号时，其频率可高达 500MHz 以上，传输距离可达 100km。但在传送数字信号时，需要在接口处安装一个电子设备，用以把进入网络的数字比特流转换为模拟信号，把网络输出的模拟信号转换成比特流。

由于在宽带系统中要用到放大器来放大模拟信号，而放大器仅能单向传输信号，因此在宽带电缆的双工传输中，一定要有数据发送和数据接收两条分开的数据通路。

1.2.6.3　光纤

光纤就是能导光的玻璃纤维，利用光纤传递光脉冲进行通信就是光纤通信，有光脉冲表示比特 1，无光脉冲表示比特 0。光纤具有如下显著特点：

（1）光纤直径很小，只有 0.1mm 左右，因而重量轻。

（2）传输损耗小，中继距离长，对远距离传输特别经济。

（3）由于可见光的频率非常高，约为 10^8MHz 的数量级，因此一个光纤通信系统的传输带宽远远大于目前其他各种传输介质的带宽。

（4）不受电磁干扰、防腐和不会锈蚀。

（5）不怕高温，防爆、防火性能强。

（6）无串音干扰，保密性好。

（7）光纤的主要缺点是将两根光纤精确地连接需要专用设备。

光纤按传输方式可分为多模光纤和单模光纤。

1. 多模光纤

多模光纤是利用光的全反射特性来导光的。若光从光密媒质射向光疏媒质，则折射角大于入射角。如果不断增大入射角可使折射角达到 90°，这时的入射角称为临界角。如果继续增大入射角，则折射角会大于临界角，使光线全部返回光密媒质中，这种现象称为光的全反射。根据这一原理，光纤主要由纤芯和包层构成，纤芯的折射率高，包层的折射率低，如图 1-34 所示。

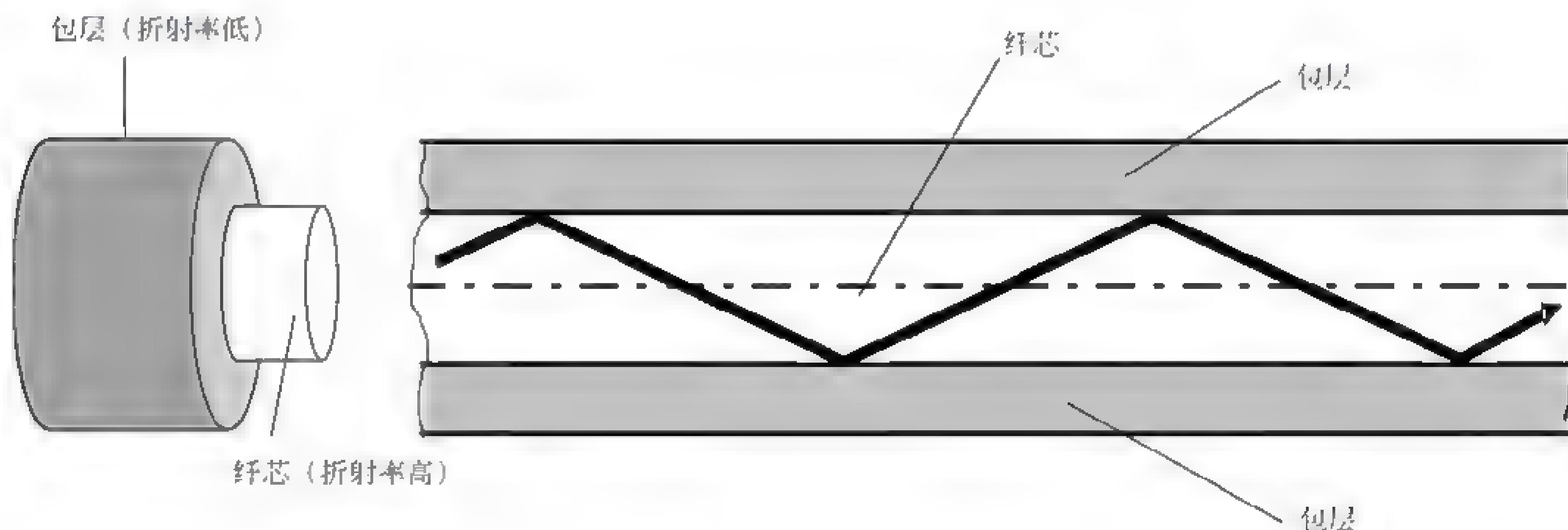


图 1-34 光纤的结构

多模光纤的光源为发光二极管，发出的可见光定向性较差，光以不同的角度进入纤芯。实际上，只要从纤芯中射到纤芯表面的光线的入射角大于某一个临界角，就可产生全反射，因此，存在许多条不同角度入射的光线在一条光纤中传输，如图 1-35 所示。光脉冲在多模光纤中传输时会逐渐展宽，造成失真，因此多模光纤只适合于近距离传输。

为了克服多模光纤的缺点，出现了梯度型多模光纤。根据经过媒体的光密越小，光传播越快的特性，梯度型多模光纤纤芯的折射率从中间往边缘逐渐变小，光在其中传输的路径变成了曲线，如图 1-36 所示。

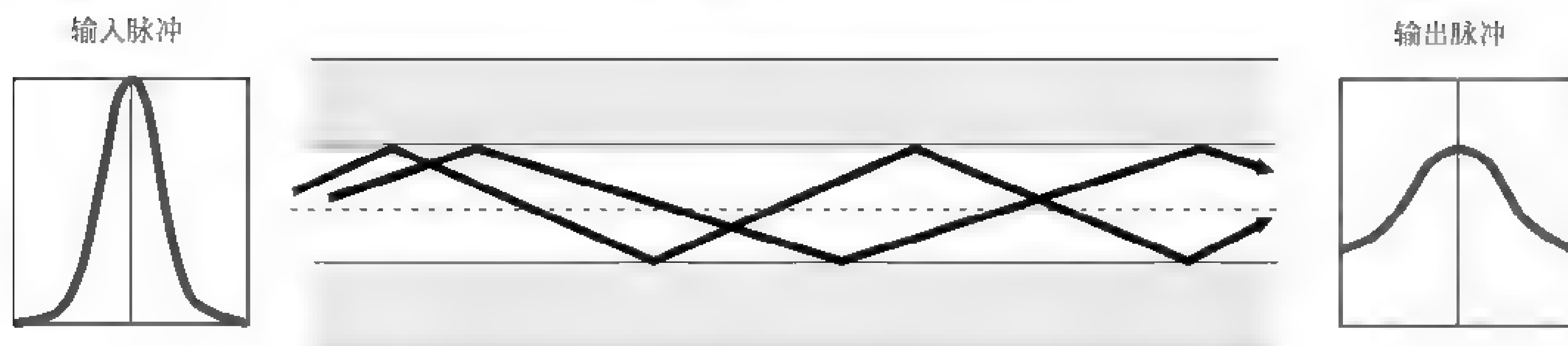


图 1-35　多模光纤

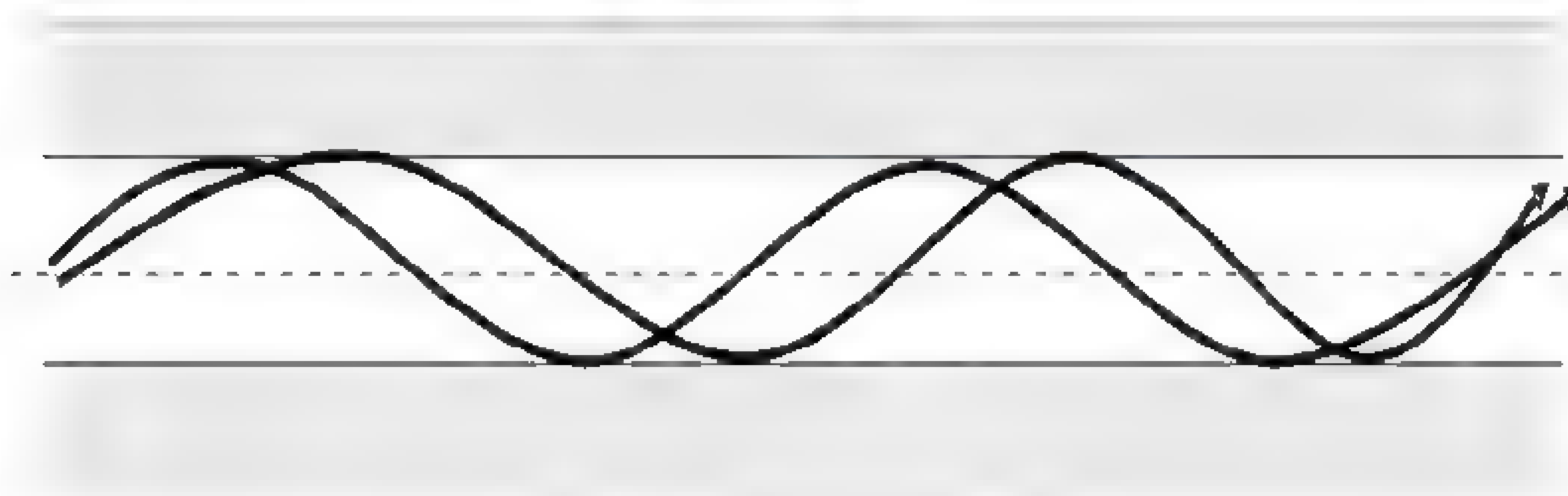


图 1-36　梯度型多模光纤

2．单模光纤

如果光纤的直径减小到只有一个光的波长大小，则光纤就像一根波导那样，它可使光线沿直线传播，而不会产生多次反射。单模光纤就是按这样的原理制成的，如图 1-37 所示。单模光纤的纤芯很细，直径只有几微米，制造成本较高。同时，单模光纤的光源使用定向型很好的激光二极管。因此，单模光纤的损耗较小，传输距离远。

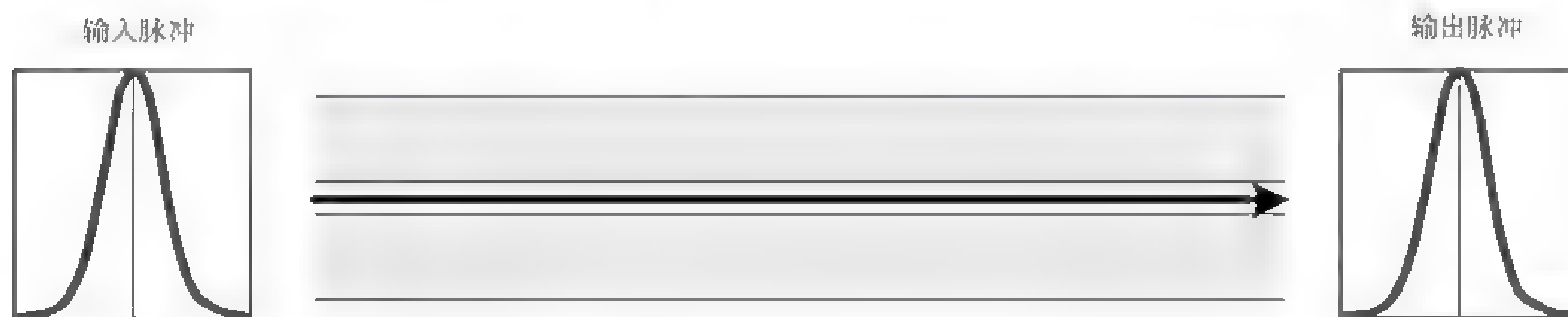


图 1-37　单模光纤

光纤有三种连接方式。首先，可以将它们接入连接头并插入光纤插座；其次，将两根切割好的光纤的一端放在一个套管中，然后钳起来，让光纤通过结合处来调整；第三，两根光纤可以被融合在一起形成坚实的连接。

由于光纤很细，连包层一起的直径也不到 0.2mm，因此必须将光纤做成很结实的光缆。一根光缆少则只有一根光纤，多则可包括数十至数百根光纤，再加上加强元件和填充物就可以大大提高其机械强度，最后加上包带层和外护套，就可以使抗拉强度达到几

公斤，完全可以满足工程施工的强度要求。

1.2.6.4 陆地微波

微波是指频率在 0.3GHz～300GHz 范围的电磁波，陆地微波通信就是利用此频段的电磁波来传递信息，目前主要是使用 2GHz～40GHz 的频率范围。

陆地微波系统的主要用途是完成远距离远程通信服务和楼宇间建立短距离的点对点通信。与其他传输介质相比，微波具有如下特点：

（1）微波波长短，接近于光波，在空间主要是直线传播，而地球表面是个曲面，微波会穿透电离层而进入宇宙空间，因此传播距离受到限制，必须设立中继站增大传输距离。

（2）微波频率高，频段范围也很宽，因此通信信道的容量大。

（3）因为工业干扰和天电干扰的主要频谱成分比微波频率低得多，因而微波传输质量较高。

（4）由于波长短，天线尺寸可做得很小，通常做成面式天线，增益高，方向性强。

（5）与相同容量和长度的电缆载波通信比较，微波接力通信建设投资少，见效快。

（6）微波无法穿透障碍物，因此相邻微波站之间必须直视，距离不会太远，一般为 50km。

（7）微波的损耗与距离和波长有关，可由下式表达：

$$L = 10\lg\left(\frac{4\pi d}{\lambda}\right)^2 \text{dB}$$

其中 d 是天线间的距离，λ是波长。

（8）微波在空间会发散，某些微波可能被较低的大气层或障碍物折射，从而比直线传播的微波多走一段距离，产生多路衰减。

（9）微波的传播有时会受到恶劣气候的影响。

1.2.6.5 卫星微波

卫星微波是陆地微波的发展，利用人造地球卫星作为中继站，转发微波信号，在多个微波站或称地球站之间进行信息交流。卫星微波通信已经广泛用于长途电话通信、蜂窝电话、电视传播和其他应用。

卫星从上行链路接收传输来的信号，将其放大或再生，再从下行链路上发送。但是卫星必须在空中移动，卫星落下水平线后，通信就必须停止，一直到它重新在另一个水平线上出现。采用同步卫星能保证持续的进行传输，因为同步卫星与地球保持固定的位置，它位于赤道轨道，离地面 35 784km。三颗相隔 120°的同步卫星几乎能覆盖整个地球表面，基本实现全球通信。

卫星微波与陆地微波相比，具有以下特点：

（1）卫星通信的距离远，且通信费用与通信距离无关。

（2）卫星微波具有广播性质。

（3）卫星信道的传播时延较大。

1.2.6.6　无线电

无线电波很容易产生，可以传播很远，容易穿过建筑物，可以被电离层反射，因此被广泛用于通信，不管是室内还是室外。无线电波同时还是全方向传播的，因此发射和接收装置不必在物理上很准确的对准。

无线电波的特性与频率有关。在较低频率上，无线电波能轻易地通过障碍物，但是能量随着与信号源距离的增大而急剧减小。在高频上，无线电波趋于直线传播并受障碍物的阻挡，还会被雨水吸收。在所有频率上，无线电波易受发送机和其他电子设备的干扰。

由于无线电波能传得很远，用户间的相互串扰就是个大问题，所以，所有的政府都控制对用户使用发射器的授权。

1.2.6.7　红外线

红外线的主要特点是不能穿透坚实的物体，这意味着一间房屋里的红外系统不会对其他房间里的系统产生干扰，而其放窃听的安全性要比无线电系统好。所以使用红外系统不需要政府授权。

红外通信使用调制非相干红外线光的收发机进行，收发机互相置于视线内对准，直接或经房间天花板的浅色表面的反射传递信息，被广泛用于短距离通信。电视、录像机使用的遥控装置都利用了红外线装置。红外线具有方向性、便宜并且容易制造，也成为室内无线网的候选对象。

1.2.7　检错与纠错

在数据传输过程中，由于信道受到噪声或干扰的影响，信号的波形传到接收方就可能会发生错误。为了把这些错误减少到人们预期要求的最低限度，就需要进行差错控制。

差错控制的原理很简单。在被传送的 k 位信息后附加 r 位冗余位，被传送的数据共 $k+r$ 位，而这 r 位冗余位是用某种明确定义的算法直接从 k 位信息导出的，接收方对收到的信息应用同一算法，将结果与发送方给它的结果进行比较，若不相等则数据出现了差错。如果接收方知道有差错发生，但不知道是怎样的差错，然后向发送方请求重传，这种策略称为检错。如果接收方知道有差错发生，而且知道是怎样的差错，这种策略称为纠错。

1．二维奇偶校验

二维奇偶校验基于一维的奇偶校验，除了把额外的 1 个比特附加到 7 个比特编码上

来平衡字节中1的个数外，还对数据中每一字节的每一比特位置进行类似的计算，产生一个额外的奇偶校验字节。如图1-38所示的例子，对42位数据进行二维偶校验，产生6个字节数据和一个奇偶校验字节，加入了14位的冗余信息。

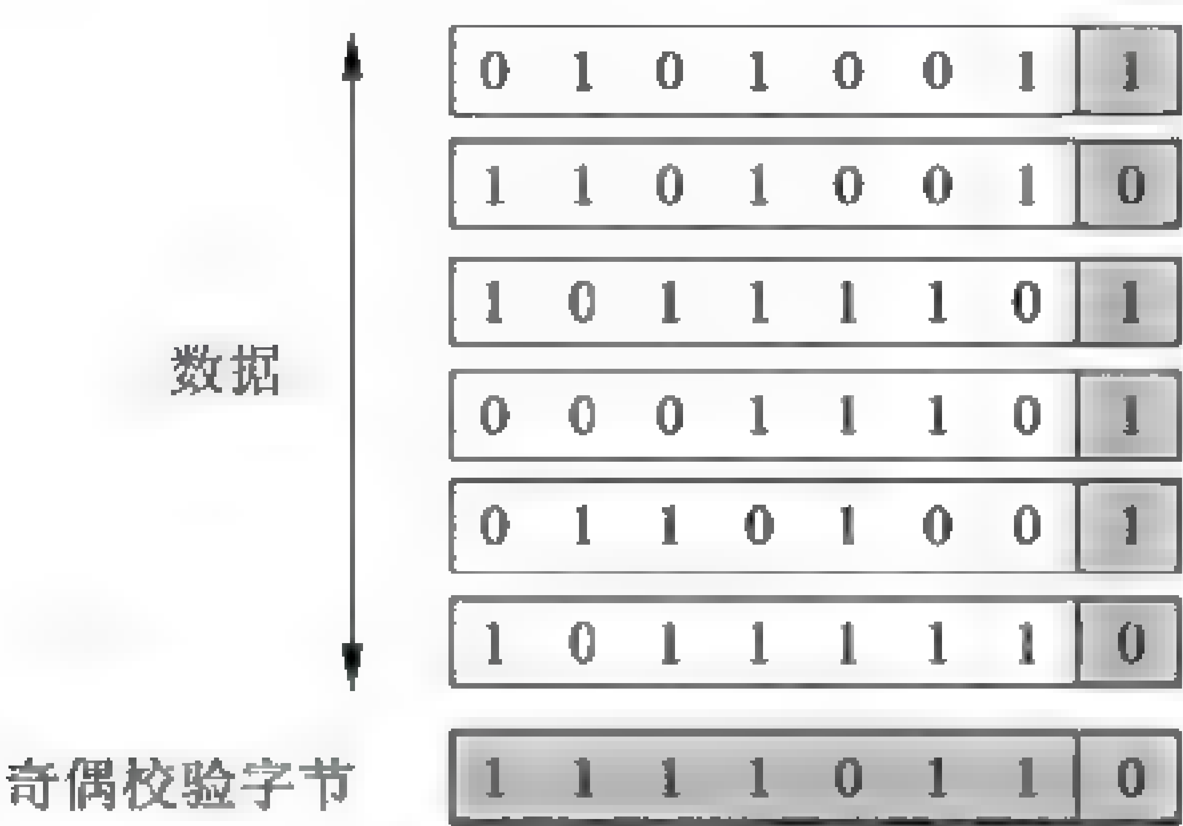


图1-38 二维偶校验

2．循环冗余校验

循环冗余校验（Cyclic Redundancy Check，CRC）是一种通过多项式除法检测错误的方法，将每个比特串看作一个多项式，采用模2运算。通常它将比特串

$$b_{n-1}b_{n-2}b_{n-3}\cdots b_2b_1b_0$$

解释成多项式

$$b_{n-1}x^{n-1}+b_{n-2}x^{n-2}+b_{n-3}x^{n-3}+\cdots+b_2x^2+b_1x^1+b_0x^0$$

如果采用多项式编码的方法，发送方和接收方必须事先商定一个生成多项式 $G(x)$，生成多项式的高位和低位必须是1。以下4个生成多项式已成为国际标准。

CRC-12 ：$x^{12}+x^{11}+x^3+x^2+x+1$

CRC-16 ：$x^{16}+x^{15}+x^2+1$

CRC-CCI ：$x^{16}+x^{12}+x^5+1$

TT

CRC-32 ：$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$

对 m 位的数据 $M(x)$，要进行循环冗余校验，发送方的处理过程如下：

（1）设 $G(x)$为 r 阶，在数据的末尾附加 r 个0，使数据为 $m+r$ 位，则相应的多项式 $B(x)=x^rM(x)$。

（2）按模2除法用对应于 $G(x)$的位串去除对应于 $B(x)$的位串，求出余数 $R(x)$。

（3）按模2减法从对应于 $B(x)$的位串中减去余数，结果就是要传送带循环冗余校验的帧 $T(x)=B(x)-R(x)$。

如图1-39所示的例子，帧为1101011011B，所选的生成多项式 $G(x)=x^4+x+1$，则 $r=4$，在帧后附加4个0。

```
帧：    1101011011
除数：  10011
                         1 1 0 0 0 0 1 0 1 0
              ------------------------------
1 0 0 1 1   | 1 1 0 1 0 1 1 0 1 1 0 0 0 0
              1 0 0 1 1
              ---------
                1 0 0 1 1
                1 0 0 1 1
                ---------
                  0 0 0 0 1
                  0 0 0 0 0
                  ---------
                    0 0 0 1 0
                    0 0 0 0 0
                    ---------
                      0 0 1 0 1
                      0 0 0 0 0
                      ---------
                        0 1 0 1 1
                        0 0 0 0 0
                        ---------
                          1 0 1 1 0
                          1 0 0 1 1
                          ---------
                            0 1 0 1 0
                            0 0 0 0 0
                            ---------
                              1 0 1 0 0
                              1 0 0 1 1
                              ---------
                                0 1 1 1 0
                                0 0 0 0 0
                                ---------
                                  1 1 1 0
余数：  1110

              1 1 0 1 0 1 1 0 1 1 0 0 0 0
                                  1 1 1 0
              ---------------------------
              1 1 0 1 0 1 1 0 1 1 1 1 1 0

传输的帧：11010110111110
```

图 1-39　循环冗余校验码的计算

很显然，$T(x)$能被 $G(x)$除尽。因此当接收方收到的比特流相应的多项式为 $T'(x)$时，接收方将 $T'(x)$除以 $G(x)$，若余数为 0，则接收方认为 $T'(x)=T(x)$，否则接收方认为发生

了错误并要求重传。

3．检错重发（Automatic Repeat reQuest，ARQ）

检错重发方式中，发送端经信道编码后可以发出具有检错能力的码组，接收端收到后经检测如果发现传输中有错误，则通过反馈信道把这一判断结果反馈给发送方，然后发送端把前面发出的信息重新传送一次，直到接收端认为已经正确为止。常用的检错重发系统有停发等候重发、返回重发和选择重发三种。

1）停发等候重发

停发等候重发系统的发送端在某一时刻向接收端发送一个码组，接收端收到后经检测若未发现传输错误，则发送一个确认信号（ACK）给发送端，发送端收到 ACK 信号后再发送下一个码组；如果接收端检测出错误，则发送一个否认信号（NAK），发送端收到 NAK 信号后重发前一个码组，并再次等待 ACK 或 NAK 信号。这种方法效率不高，但工作方式简单。

2）返回重发

在返回重发系统中，发送端无停顿地送出一个又一个码组，不再等待 ACK 信号，一旦接收端发现错误并发回 NAK 信号，则发送端开始重发检测出错误的码组以及该错误码组之后的码组。

3）选择重发

在选择重发系统中，发送端也是连续不断地发送码组，接收端发现错误发回 NAK 信号。与返回重发系统不同的是，发送端不是重发前面的所有码组，而是只重发有错误的那一组。显然，这种选择重发系统传输效率最高，但控制最复杂。

1.3 网络体系结构

计算机网络是一个复杂的系统，通常把计算机网络按照一定的功能与逻辑关系划分成一种层次结构。这种层次结构对用户来说是“透明”的，用户不用关心网络是如何工作的。但是作为网络研究人员就要知道这种层次关系及其实现的功能。除了计算机网络的层次关系，计算机网络中通常有很多节点，这些节点在计算机之间需要相互交换数据，交换数据时必须遵守的一组约定或规则称为协议。计算机网络的体系结构就是这种层次结构与协议的集合。

网络协议是计算机网络体系结构的关键要素之一。协议包含三个要素：语法、语义和时序。语法是数据与控制信息的结构或格式。语义是需要发出何种控制信息、执行何种动作或返回何种应答。时序关系是事件实现顺序的详细说明。协议与计算机的网络层次结构相对应。协议体系结构的思想是：用一个构造好的模块集合来完成不同的通信功能。

OSI 参考模型是计算机网络的基本体系结构模型。依据网络的不同，通常使用的协

议有 TCP/IP 协议、IPX/SPX 协议、NetBEUI 协议。其中，TCP/IP 协议在 Internet 中使用，是目前应用范围最广的协议，实现各种不同的计算机网络平台间的互相连接和通信。

1.3.1　应用层

1．应用层功能

网络的应用层是网络体系结构中的最高层，它是计算机开放互连环境与本地系统的操作环境和应用系统直接接口的一个层次。在功能上，应用层为本地系统的应用进程（Application Process，AP）访问网络环境提供手段，也是唯一直接给应用进程提供各种应用服务的层次。即借助应用实体、应用协议和应用服务实现端点用户之间的信息交换。

需要说明的是，在 OSI 参考模型中定义的应用层中不包含应用系统，应用层的含义是“直接为用户的应用进程提供服务”的一个 OSI 功能层。但在很多实际的计算机网络系统（如 Internet 的 TCP/IP）中，应用层是 OSI 环境下的应用服务与应用系统的融合体，它的应用层协议就是一个个具体的应用协议，并表现为一个个具体的应用程序，如文件传输程序 FTP、远程终端程序 Telnet 等。

应用层的主要功能如下。

（1）应用管理：由应用管理实体对应用进程进行管理，包括应用进程参数初始化，应用进程的创建、维护和终止，给应用进程分配资源和收回资源等。

（2）系统管理：包括开放系统中资源的激活、维持和终止，开放系统参数的初始设置和修改，管理实体间连接的建立、维持和释放，出错检测及诊断等。

2．应用层实现模型

计算机网络的最终目的是为现实的应用系统（更确切的说是应用进程）创建一种开放的互连通信环境（即 OSI 环境），并提供本地系统与外界系统进行应用合作的各种应用服务。实际应用系统中，当与远端的应用系统进行交互时，应用进程除与 OSI 环境进行交互外，还与本地系统交互。以本地应用进程 A 同另一端系统中 B 应用进程发送一个文件为例，进程 A 在发送前首先要通过本地系统找到该文件（与 OSI 无关的交互），然后发给应用进程 B（与 OSI 有关的交互）。

在 OSI 标准中，把应用进程中与 OSI 有关的那部分抽象为应用实体（Application Entity，AE），并放入应用层内，用以代表应用进程参与和其他应用进程的交互（执行 OSI 通信）。而把与 OSI 无关的那部分应用进程仍称为应用进程 AP，放在应用层之外。应用实体可与下层（OSI 的表示层）进行联系。应用层实现模型如图 1-40 所示。

通常一个应用实体由一个用户元素（User Element，UE）和若干应用服务元素（Application Service Element，ASE）组成。UE 是应用进程（AP）与应用实体之间的接口，应用进程通过 UE 取得应用层的服务。在具体的实系统中，UE 通常体现为一组服务

调用。应用服务元素 ASE 是一些可重复使用的程序模块，这种模块提供某种应用 OSI 的能力。两个对等应用实体之间执行某种应用层协议向其服务用户提供某种服务。

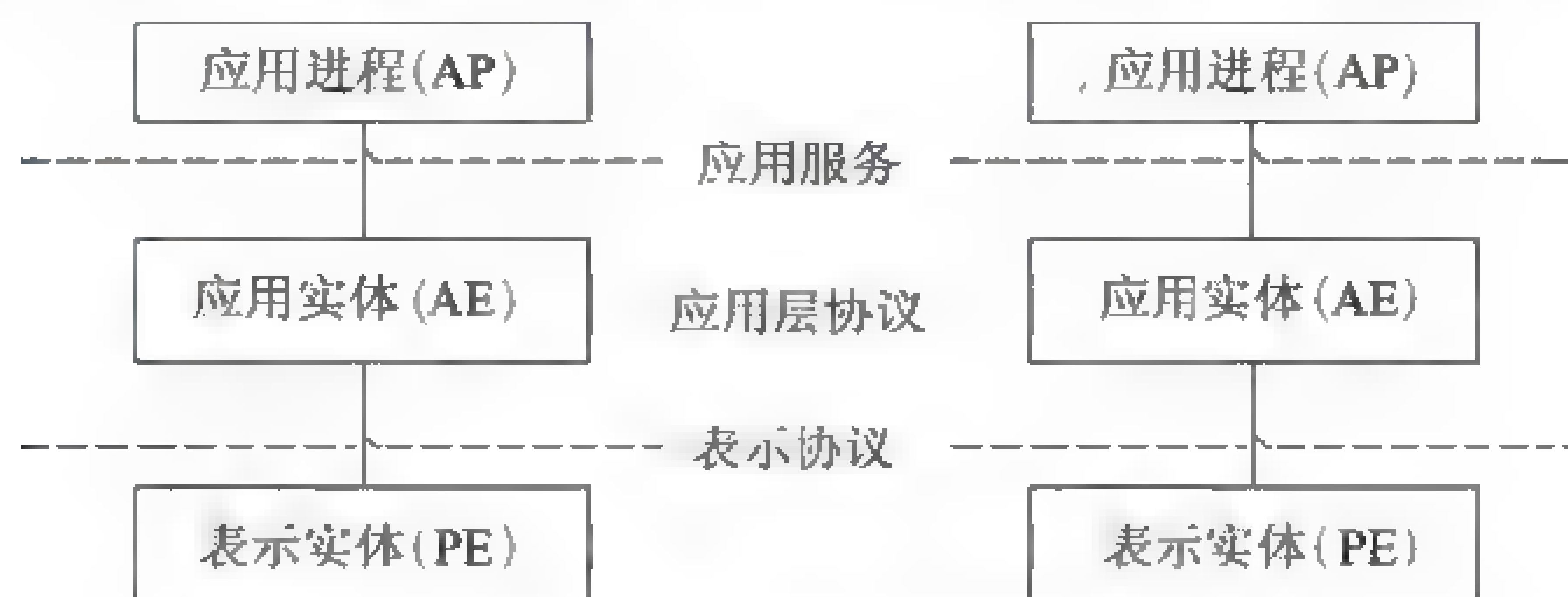


图 1-40 应用层实现模型

1.3.2 传输层

1.3.2.1 传输层的主要功能

传输层是网络体系结构中最关键的一层，是资源子网和通信子网的界面与桥梁，它是面向应用的高层和面向通信的低三层协议之间的接口。传输层主要具有以下功能。

（1）连接管理：传输层连接的管理包括端到端连接的建立、维持和拆除。传输层可同时支持多个进程的连接，即将多个进程连接复用在一个网络层连接上。

（2）优化网络层提供的服务质量：传输层优化网络服务质量包括检查低层未发现的错误、纠正低层检测出来的错误、对接收到的数据包重新排序、提高通信可用带宽、防止无访问权的第三者对传输的数据进行读取或修改等。

（3）提供端到端的透明数据传输：传输层可以弥补低层网络所提供服务的差异，屏蔽低层网络的细节操作，对数据传输的控制包括数据报文分段和重组、端到端差错检测和恢复、顺序控制和流量控制等。

（4）多路复用和分流：当传输层用户进程的信息量较少时，将多个传输连接映射到一个网络连接上，以便充分利用网络连接的传输速率，减少网络连接个数。

1.3.2.2 传输层服务质量

传输层位于低层和高层之间，起到从通信到应用间的桥梁作用。它通过补充和完善通信子网服务质量的差异和不足，向其高层提供统一服务质量的透明数据传输服务。传输层向上层提供的服务是利用网络层服务来实现的。不同的通信子网所提供的网络服务质量是不一样的。这里的服务质量主要是指差错率。因为无论何种网络，传输层都要向高层提供同样的服务，所以，如果通信子网的服务质量好，传输层所具有的功能就可以相应的少，反之，则多。

通信子网按服务质量的不同可分为 A，B，C 三种类型。

1）A 型网络

A 型网络具有可接受的残留差错率和可接受的故障通知率，残留差错率是指未纠正的差错，故障通知率是指网络层检测到的并通知传输实体予以纠正的故障。这种网络提供近乎可靠的网络服务，当分组在网络中传输时，既不丢失、重复，也不失序。虚电路服务属于 A 型服务。公用广域网很少具有这种性能。

2）B 型网络

B 型网络具有可接受的残留差错率和不可接受的故障通知率。B 型服务较差，利用该网络的传输层必须提供差错恢复功能。X.25 分组交换网等广域网所提供的服务属于 B 型服务。

3）C 型网络

C 型网络具有不可接受的残留差错率。因为这种网络不能检测到差错，因此运行在这种网络上的传输层协议不仅要能检测到差错，而且要有差错恢复能力。数据报服务的网络或无线分组交换网络均属于 C 型服务。

由此可见，网络服务质量的划分是以用户要求为依据的。若用户要求比较高，则一个网络可能归于 C 型；反之，则一个网络可能归于 B 型甚至 A 型。例如，对于某个电子邮件系统来说，如果网络每周丢失一个分组，那么此网络也许可算做 A 型；而此网络对银行系统来说则只能算作 C 型了。三种类型的网络服务中，A 型网络服务质量最高，B 型网络服务质量次之，C 型网络服务质量最差。

1.3.2.3　寻址

传输层要在用户进程之间提供可靠和有效的端对端服务，必须把一个目标用户进程和其他的用户进程区分开来，这是由传输地址来实现的。目标用户需要这样的说明：用户标识、传输实体、主机地址和网络号码。传输层定义一组传输地址，以供通信选用。传输地址用术语“传输服务访问点”（Transport Service Access Point，TSAP）来描述。为确保所有传输地址在整个网上是唯一的，传输地址规定由网络号、主机号以及由主机分配的端口组成。

传输地址的构成有以下两种方法。

1）层次地址

该地址由一系列域组合而成，把它们从空间上分开。例如：

地址=<国家><网络><主机><端口>

这种方法的优点是路径选择方便，建立新接口也比较方便，而且不受高位编码的制约。其缺点是进程移动不方便，因原地址在新机器上不能用，故路径选择缺乏灵活性。

一个实际例子是，在 Internet 中用<IP 地址><端口号>表示 TSAP。

2）平面地址空间

平面名称对应于地理上或任何其他层次方面都无特定关系的传输地址，可以用一个号码当作单一系统内的地址。用这种方法确定的地址是唯一的，而且同它所处的位置无关。

这种方法的优点是移动进程能携带地址，单路径选择较困难、分配地址较复杂，因为要确保每个地址都是唯一的。

1.3.2.4 建立与释放连接

传输服务有两大类：面向连接的传输服务和无连接的传输服务。无连接的传输服务比较简单，不需要进行传输控制。而对于面向连接传输服务的两个用户（或进程）进行相互通信，一般要经历三个过程：建立连接、数据传输和释放连接。

1. 建立连接

首先在两个传输服务用户之间要建立连接，然后才能在该连接上进行实质性的数据传输。此传输连接应由双方的传输地址构成。在连接建立过程中，根据用户对服务质量的要求，相互协商服务的功能与参数，如选择合适的网络服务、协商传输协议数据单元的大小、确定是否使用多路复用和流量控制等。

一个传输实体向目的机器发送一个连接请求的传输协议数据单元（TPDU），待接收到对方连接的应答就可以建立连接了。这个过程通常称之为“二次握手”。

但当网络可能丢失、存储、出现重复分组时，这种简单的方法就不行了。为了解决这些问题，提出了三次握手的方法。三次握手时建立连接需要三个步骤：

（1）甲方发送一个连接请求包到乙方。

（2）乙方回送一个连接请求包到甲方。

（3）甲方再回送一个包确认验证。

2. 数据传输

一旦连接建立，两个对等实体就可以使用发送（SEND）和接收（RECIVE）原语交换数据了；如果用户的数据超过了最大分组尺寸，发送方传输层实体会将数据分段，每一个分段都有一个序列号，最后的分段有一个结束标志，这样，在接收方就能按照正确的顺序还原数据。

3. 释放连接

释放传输连接包括对称释放（正常释放）和非对称释放（突发性终止）两种情况，后者指拒绝建立连接或单方面终止连接，因为这种情况非常突然，可能会导致数据丢失，因而不适于在运输层使用。

对称释放方式在两个方向上分别释放连接，一方释放连接后，只是不能发送数据，但可以继续接收数据。

1.3.2.5　流量控制与缓冲策略

传输服务为保证连接的可靠性，需要对连接进行管理，流量控制是连接管理的基本内容之一。缓存是实行流量控制的必要措施。

传输层中流量控制是端到端执行的，可能作用在多条链路上。传输层需要解决的是端到端的流量控制问题，首先是对发送端传送实体发向接收端实体的数据流加以控制，使其不超过接收端所能承受的接收能力。在数据链路层协议中，各帧在发送端路由器和接收端路由器中被缓存起来。在传输层就要开辟很多缓冲区，造成资源浪费。一个解决方案是：根据连接所传输的信息的类型，采取源端缓冲方案和目的端缓冲方案；即对于低速突发性的信息，最好在发送端进行数据缓存；对于高速平稳的信息传输，最好在接收端进行数据缓存。

端到端的流量控制问题不仅要考虑接收方的缓存容量问题，还要考虑子网的运载问题。如果发送端发送数据太快，就会造成子网的拥塞，使用滑动窗口的流量控制方法来解决此问题。发送端动态调整窗口大小以匹配网络的运载容量。为了定期调整窗口的大小，发送端应该监测网络的运载容量和循环时间这两个参数，然后计算所希望的窗口大小。运载容量可以简单地通过计算在某段时间间隔内确定的 TPDU 数除以时间间隔来决定。循环时间包括传输、传播、排队、在接收方的处理以及确认帧的返回时间。网络的容量依赖于其数据传输量，因此应该频繁地调整窗口大小以适应网络运载容量的变化。

1.3.2.6　传输服务原语

服务在形式上是以一组原语（primitive）来描述的。原语被用来控制服务提供者采取某些行动，或报告某同层实体已经采取的行动。在 OSI 参考模型中，服务原语划分为 4 种：

1）请求（request）

用户利用它要求服务提供者提供某些服务，如建立连接或发送数据等。

2）指示（indication）

服务提供者执行一个请求以后，用指示原语通知收方的用户实体，告知有人想要与之建立连接或发送数据等。

3）响应（response）

收到指示原语后，利用响应原语向对方做出反应，例如同意或不同意建立连接等；

4）确认（confirm）

请求对方可以通过接收确认原语来获悉对方是否同意接受请求。原语可以携带参数，如连接请求原语的参数包括机器连接需要什么服务类别等。连接指示原语的参数包含呼叫者的表示、需要服务的类别等。被呼叫实体可以在响应原语中的参数里表示同意或不同意连接，若同意，则对某些参数给出协商值，比如最大数据吞吐量等；ISO 定义的传

输服务包括了 4 种类型共 10 个传输服务原语。

1.3.3 网络层

网络层是通信子网的最高层，是高层与低层协议之间的界面层。网络层用于控制通信子网的操作，是通信子网与资源子网的接口。网络层关系到通信子网的运行控制，决定了资源子网访问通信子网的方式。

1. 网络层主要功能

设置网络层的主要目的就是为报文分组以最佳路径通过通信子网到达目的主机提供服务，而网络用户不必关心网络的拓扑结构与使用的通信介质。网络层的主要功能如下。

（1）网络连接功能：网络层实体作为数据链路层服务用户，利用各条链路上的数据链路连接服务，来为传送实体之间建立端到端的网络连接关系。其中，涉及到数据通路的建立、维护和拆除的过程。

（2）路由选择功能：路由选择是为建立数据通路服务的一种功能。也就是为在源/宿节点之间建立通路而提供一些控制的过程。这些控制过程由路由算法来实现。

（3）拥塞控制功能：拥塞控制的主要功能是对进入网络的数据流实施有效控制，使通信子网避免发生“网络拥塞”和“死锁”现象，保持稳定运行。

（4）数据传输功能：在网络连接建立之后，网络层实体要为上层递交下来的数据提供传输与中继功能。根据通路的类型，传送服务数据可能在一个子网内进行，也可能要跨越互连设备进行中继转发。传输过程包括对数据的分组、排序以及进行差错和速度控制等。

根据网络连接类型的不同，网络层协议往往提供两种明显不同的数据传输方式：面向连接的虚电路方式和无连接的数据报传输方式，它们分别向上提供两类不同特征和服务质量的数据传输服务。

（5）其他功能：除了具有以上功能外，网络层还提供诸如子网接入、网络连接复用、计费以及在网络互连环境下的协议转换等功能。

2. 数据报与虚电路子网

网络层的内部构造指的是网络层内部是如何工作的。有两类构造通信子网的方法，即面向连接和无连接的方法。从通信子网内部操作的角度看，通常称连接为虚电路（Virtual Circuit，VC），类似于电话系统建立的物理电路。采用面向连接方法构造的通信子网称为虚电路通信子网。采用无连接方法构造的通信子网称为数据报通信子网。经数据报通信子网传送的是独立选路的分组，称为数据报（datagram），与普通邮件相似。

出现这两种服务方式的原因是，网络层设计者中的一个集团（以 Internet 委员会为

代表）认为：通信子网的工作是在网上传送比特，除此之外，别无他事。按照他们的观点，不管怎样设计，通信子网注定是不可靠的。因此，主机必须进行差错控制和流量控制，而不是交给网络。结论是：网络层不必再设置分组排序和流量控制等功能，提供的服务是无连接方式。另一个集团（以电信公司为代表）认为：通信子网应该提供一种可靠的、面向连接的服务。面向连接和无连接两种服务方式之间争论的实质，就是将复杂的控制功能放在何处的问题。在面向连接的服务中，它们被置于网络层（通信子网，如 ATM 网），在无连接的服务中，则被置于传输层（主机，如 Internet）。

虚电路常用于其服务方式是面向连接的子网中（如 ATM 上的 ATM AAL1）。数据报常用于其服务方式是无连接的子网中（如 IP 之上的 UDP）。但也有另外两种应用，即无连接方式的虚电路子网（如 ATM 上的 IP 或 IP 上的用户数据报协议 UDP）和面向连接方式的数据报子网（如 IP 之上的 TCP）。

1.3.4　数据链路层

数据链路层是 OSI 模型的第 2 层，它介于物理层与网络层之间。用于在相邻节点间建立数据链路，传送以帧为单位的数据，使其能够有效、可靠地进行数据交换。本层通过差错控制、流量控制等，将不可靠的物理传输信道变成无差错的可靠的数据链路。将数据组成适合正确传输的帧形式的数据单元，对网络层屏蔽物理层的特性和差异，使高层协议不必考虑物理传输介质的可靠性问题，而把信道变成无差错的理想信道。

1.3.4.1　数据链路层主要功能

数据链路层利用物理层提供的位串传输功能，在相邻节点之间实现透明的、高可靠性的数据传输。所谓透明数据传输，指无论所传数据是什么样的比特的组合，都能够照原样传输到目的节点，其处理过程对上层是不可见（透明）的。

为了完成这一任务，数据链路层应具备以下几项功能。

1）帧同步

在数据链路层，数据的传送单元是帧。帧同步是指接收方能够从所收到的比特流中准确地区分帧的起始与终止。帧是一种包括数据、控制、校验、起始与结束码在内的组织结构，能够使接收方明确帧的格式和有效的识别传输中的差错。在数据链路层中，由于数据是以帧为单位一帧一帧地传输，因此，当接收方识别出某一帧出现错误时，只需重发此帧而不必将全部数据进行重发。

2）链路管理

链路管理包括链路的建立、维护和释放。

链路管理就是犹如甲、乙双方打电话。在甲、乙双方通话前，首先必须通过交换一些必要的信息，确认受话方已准备好接电话；在甲、乙双方通话过程中要保持通话链路始终为“通”状态；当通话双方通话完毕后要释放链路，也就是释放连接。

3）差错控制

在链路传输帧的过程中，由于种种原因不可避免的会出现帧传错或帧丢失的情况，系统必须能够对差错进行及时的控制及恢复。

4）流量控制

在数据传输过程中，如果对信息流量控制不好就会产生严重的过载和阻塞情况，以至数据传输不能正常进行。为了使信息在网络中尽可能快地和均匀地流动，就要对通信流量进行控制。

数据链路层流量控制的目的就是要避免阻塞和在发生阻塞的情况时能够解除阻塞。其实质是进行调节、控制网络内部信息的流动，即控制相邻两个节点之间数据链路上的流量。

产生阻塞的主要原因如下：

① 当一个发送信息的机器相对于接收信息的机器来说，以过快的速率进行信息传送时，接收机的缓冲区无法处理这样快的传输，就导致阻塞。

② 当一个工作站突然发送大量的数据给另一个工作站时，会产生阻塞。

解决阻塞的主要方法如下：

① 通过对点到点的同步控制，来保证发送方发送数据的速度与接收方接收数据的速度相匹配。

② 控制网络的输入，避免产生一个工作站突然将大量的数据报文提交给另一工作站的现象。

③ 接收工作站在接收数据报文之前，要保留出足够的缓冲存储空间。

1.3.4.2 数据链路层成帧方法

在数据链路层，数据按帧传送，当出现差错时，可只重传有差错的帧。为此，收方应能从到达的数据流中准确地区分出各帧的边界，称为帧同步。帧同步又称为成帧。

下面介绍 4 种典型成帧方法：

1）字符计数法

字符计数法在帧头中设置一个字段以标明该帧包含的字符数。字符计数法存在的问题是，如果某帧的字符计数字段出错将导致目的方无法知道该帧的实际长度，因而目的方无法确定下一帧的开始位置，出现与发送方不同步。因此，现在已很少单独使用字符计数法。

2）带字符填充的首尾界符法

第二种成帧法避开了出错后再同步的问题，每一帧以 ASCII 字符序列的 DLE STX 开头，以 DLE ETX 结束（DLE 代表 Data Link Escape；STX 代表 Start of Text；ETX 代表 End of Text）。目的机器一旦丢失帧边界，只需查找 DLE STX 或 DLE ETX 字符序列，就可以重新找到帧边界所在的位置。

当传送如目标程序或浮点数这样的二进制数据时，DLE STX 或 DLE ETX 可能出现在数据中，因而误判帧的边界。一种解决办法是，发送方的数据链路层在数据中出现的每个 DLE 字符前插入一个 DLE，接收方则在将数据交给网络层之前删除 DLE。这种技术叫做字符填充（character stuffing），如图 1-41 所示。

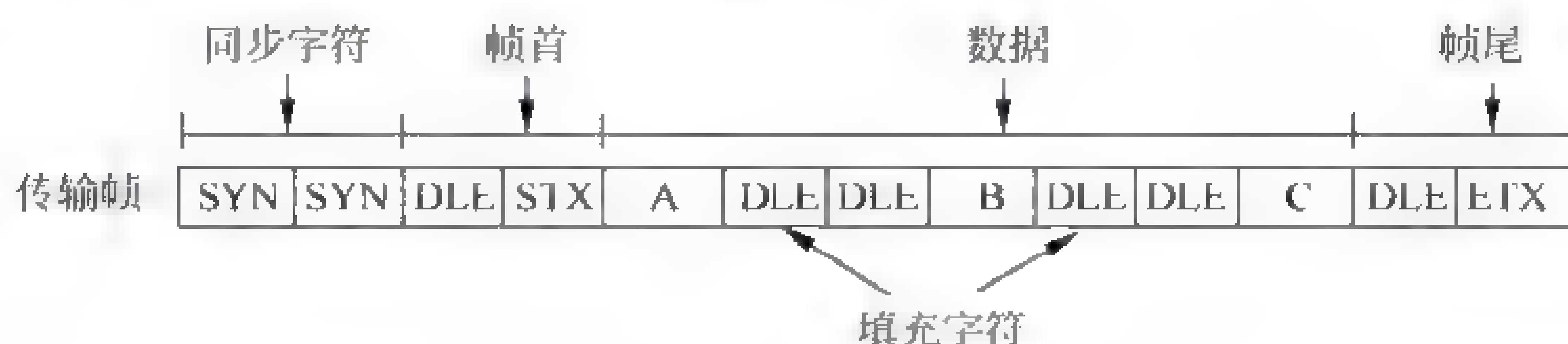


图 1-41　带字符填充的首尾界符法

这种成帧方法的主要缺点是完全依赖于特定的字符集（例如 ASCII 字符），此外，报文的长度还必须是字符长度的整数倍。

3）带位填充的首尾标志法

这种技术允许数据帧包含任意位数（在最大帧长范围内）。其工作方式如下：每一帧使用一个特殊的位模式，例如 01111110 作为开始和结束标志字节。

当发送方的数据链路层在数据中遇到 5 个连续的 1 时，就自动在其后插入一个 0。当接收方接收到 5 个连续的 1 后面跟着一个 0 时，自动将此 0 删去。这种方法使帧中的数据字段可以包含任意的位序列，称为位填充（bit stuffing）技术，如图 1-42 所示。

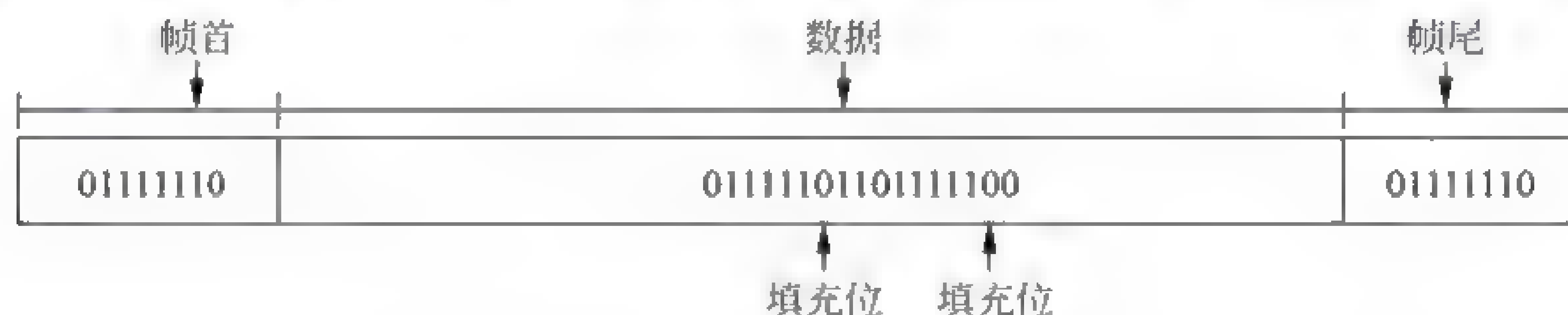


图 1-42　带位填充的首尾标志法

位填充技术和字符填充技术一样，对通信双方计算机的网络层来说都是透明的。

采用位填充技术，两帧间的边界可以通过标志字节唯一地识别。失去同步的接收方只需在输入流中扫描标志序列，即可重新获得同步。

4）物理层编码违例法

在物理线路编码（将数据用电信号的波形表示出来）方案中采用冗余技术的网络，可以采用这种成帧方法。一些局域网用两个码元译码成数据的一位。例如，采用曼彻斯特编码时，将数据位 1 编码成高-低电平对，将数据位 0 编码成低-高电平对，而高-高电平对和低-低电平对（无效物理编码）则用作帧界定符。这样，在每个数据位中都将出现电平的跳变，而用作帧界定的每个数据位中却不会有电平的跳变，接收方据此就很容易

确定帧的边界了。802.3 和 802.5 局域网标准就采用了这种方法。

很多数据链路协议为提高可靠性，采用字符计数与其他方法相结合的策略。当一个帧到达时，其计数字段被用来确定帧尾。只有当帧界定符出现在帧尾，且校验和正确时，该帧才会被接受为有效帧。否则，将继续扫描输入流直到下一个界定符。

1.3.4.3 数据链路层差错控制方法

计算机通信要求有极低的位差错率，为此，广泛采用编码技术来进行差错控制。一类是前向纠错，采用纠错码；一类是检错重发，采用检错码。

1）前向纠错

接收方收到有差错的数据帧时，能够自动将差错改正过来。这种方法开销较大，不适合于计算机通信。

2）检错重发

接收方收到有差错的数据帧时，检测到差错并让发送方重发该帧，直到接收方正确收到为止。在计算机通信中常用检错重发送方法。

为保证发送方发出的所有帧都正确有序地交付给目标机网络层，需要启动确认重传机制，由接收方向发送方提供有关接收情况的反馈信息。如果发送方收到肯定确认，则通知此帧已正确到达；若收到的是否认，则意味着需要重传此帧。

为防止帧的丢失，需设置定时器。当发送方等待足够的时间还未收到接接收方的确认帧，则可重传此帧。但重传可能导致接收方收到重复帧。为此，可为各帧编号，使接收方能辨别是重复帧还是新帧，以保证每帧最终只交付给目标机网络层一次。

目前，主要使用的检错码是奇偶校验码和循环冗余码（CRC）。

奇偶校验码分为垂直奇（偶）校验、水平奇偶校验和水平垂直奇偶校验。它们的冗余位少、方法简单，但纠错能力差，一般只用于可靠性要求较低的通信场合。

CRC 是一种能力相当强的检错码，并且实现编码和检错的电路比较简单，因而得到了广泛的应用。

1.3.4.4 基本链路控制规程

通信控制规程又称传输控制规程。它是为实现传输控制所制定的一系列规则。数据通信的过程包括 5 个阶段：线路连接、确定发送关系、数据传输、传输结束、拆线。每个阶段中都有一定的规定。所以，在通信控制规程中涉及到数据编码、同步方式、差错控制、应答方式、传输控制步骤、通信方式和传输速率等内容。

数据链路层有两个基本链路控制规程：面向字符型链路控制规程和面向比特型链路控制规程。

1．面向字符型链路控制规程

面向字符型链路控制规程规定一些特殊的非打印字符作为帧界定符，以实现发送和

接收方的同步。除帧界定符外，还需要一些其他的控制字符，如询问、确认等，总共设置了 10 个传输控制字符。

面向字符的数据链路控制规程又分为两类：一类以规定的字符作为帧的开始和结束，实现帧定界，以保证同步。另一类以帧的长度来实现帧的分界。

2．面向比特型链路控制规程

随着通信量的增加及计算机网络的应用范围不断扩大，低效率嵌进控制字符的面向字符的数据链路规程越来越变得力不从心，面向比特的数据链路控制规程解决了这个问题，其典型代表是高级数据链路控制协议（High Level Data Link Control，HDLC）。

面向比特的链路控制规程有以下特征：

（1）无论是信息报文还是控制报文均以统一的帧格式进行传输。

（2）不采用特定的控制字符实现链路两端的同步，而是采用特定的位组合实现同步。

（3）帧中的数据和控制信息完全独立，除标志外，所有信息均不受任何位组合的限制，具有良好的透明性。

（4）在链路上传输信息采用连续发送方式，即发送一帧后，无须等待对方的应答就可以发送下一帧，提供了信息传送效率。

1.3.4.5　数据链路层协议

数据链路层协议中最有代表性的是高级数据链路控制协议（HDLC）。

HDLC 是面向比特的数据链路控制规程。HDLC 协议具有透明传输、可靠性高、传输效率高和灵活性强等特点。HDLC 协议规定了数据传输的操作模式、数据帧格式、帧类型等等。

为满足不同应用场合的需要，HDLC 协议定义了三种站类型、两种链路结构和三种数据响应模式。

1．通信站类型

HDLC 协议允许有三种类型的通信站：主站、从站和复合站三类。

（1）主站：主站负责控制链路的操作与运行。主站向从站发送命令帧，并从从站接收响应帧。在多点链路中，主站负责管理与各个从站之间的链路。

（2）从站：从站在主站的控制下进行工作。从站发送响应帧作为对主站命令帧的响应。从站对链路无控制权，从站之间不能直接进行通信。

（3）复合站：同时具有主站和从站的功能，既可以发送命令帧，也可以发送响应帧。

2．链路结构

HDLC 协议规定了两种链路结构：不平衡链路结构和平衡链路结构。

（1）不平衡型结构：不平衡型结构有一个主站和一个或多个从站被连在一条线路上。

（2）平衡型结构：平衡型结构由两个复合站的点对点连接构成。两个复合站都具有数据传送和链路控制能力。

3．数据响应方式

HDLC 协议有三种数据响应方式。

1）正常响应方式（NRM）

这是一种不平衡型结构的操作方式。在这种操作模式中，从站只能为了响应主站的命令帧而进行传输，从站在确切地接收到来自主站的允许传输命令后才可以开始响应传输。响应信息可以由一个或多个帧组成，同时保持占线状态，并指出哪一个是最后一帧。从站在发出最后的响应帧之后，将停止发送，直到再次收到从主站发出的确切的允许传输的命令后才能重新开始传输。在这种方式中，主站负责管理整个链路，负责对超时、重发及各类恢复操作的控制，并且有查询从站和向从站发送命令的权利。正常响应模式适用于不平衡多点探询的链路结构。

2）异步响应方式（ARM）

这是一种不平衡型结构的操作方式。在这种操作模式中，在传输帧中可以包含有信息，或者仅以控制为目的而发送的帧，由从站来控制超时和重发。异步传输可以是一帧也可以是多帧。同为不平衡型结构的操作方式，异步响应方式与正常响应方式的区别在于，异步响应方式下从站不必确切地接收到来自主站的允许传输的命令就可以开始传输。

3）异步平衡方式（ABM）

这是一种平衡型结构的操作方式。这种方式下可以传输一帧和多帧。传输是在复合站之间进行的，在传输过程中一个复合站不必接收到另一个复合站的允许就开始传输。适用于通信双方都是组合站的平衡型链路结构。

4．HDLC 帧格式

帧是数据链路上传输的基本信息单位，HDLC 协议的帧格式如图 1-43 所示。

比特	8	8	8	可变	16	8
	标志 F	地址 A	控制 C	信息 I	帧校验 FCS	标志 F

图 1-43　HDLC 的帧格式

所有的帧都使用这种标准的帧格式，每个帧包括链路控制信息和数据。链路控制信息包括帧首和帧尾的标志序列 F、地址字段 A、控制字段 C 及帧校验序列 FCS。HDLC 协议规定了长格式和短格式两种帧。长格式包括数据和链路控制信息，短格式只包含链路控制信息。

标志序列 F：是一个独特的 8 位序列（01111110），表示帧的开始和结束。它也可兼作上一个帧的结束标志和下一个帧的开始标志，具有帧同步的作用。标志序列也可用作帧间填充字符。不包括标志序列在内，如果一个帧的长度小于 32 位，则认为该帧无效。

地址字段 A：在命令帧中，给出执行该命令的次站地址；在应答帧中，该字段给出作出应答的次站地址。通常地址字段 A 为 8 位，共有 256 种编址。为了适应特定的环境，

允许采用扩充地址字段。具体办法是：保留每个 8 位地址的最低位为 0 来表示后面跟着的 8 位是该基本地址的扩充地址，扩充地址的格式与基本地址相同，依次采用上述方法可以多次对地址字段进行扩充。

控制字段 C：用于表示所使用帧的类型以及序列号。该字段也可以被用来去命令被选站执行某种操作，或传递被选站对主站命令的应答。

信息字段 I：表示链路所要传输的实际信息。它不受格式或内容的限制，任何合适的长度都可以。通常信息字段的实际长度往往与数据站设置的缓冲区有关，最大长度是通信信道差错率的函数。

帧校验序列 FCS：可以使用 16bit 或 32bit 的帧校验序列，用于差错检测。

5．HDLC 帧类型

在 HDLC 中，帧被分为以下三种。

（1）信息帧：用于传输数据的帧，具有完全的控制顺序。

（2）监控帧：用于实现监控功能的帧。包括接收准备好、接收未准备好、请求发送、选择发送等监控帧。主要完成回答、请求传输、请求暂停等功能。

（3）无编号帧：用于提供附加的链路控制功能的帧。该帧没有信息帧编号，因此可以表示各种无编号的命令和响应（一般情况下，各种命令和响应都是有编号的），以扩充主站和从站的链路控制功能。

6．HDLC 的流量控制

流量控制的目的是克服通信拥挤或阻塞现象，保证发送端的发送数据速率与接收端能够接收的数据速率相容。流量控制方法有发送等待方法、预约缓冲区法、滑动窗口控制方法、许可证法和限制管道容量法等。

7．HDLC 信息交换过程

按照 HDLC 协议，两个通信站使用交换线路的通信，可以分为 5 个阶段：建立连接、建立链路、数据传输、拆除链路和拆除连接。如果通信双方采用专线连接，则不必建立链路的连接和拆除链路的连接。

1.3.5　物理层

物理层是 OSI 参考模型的最低层，向下直接与物理介质连接。它是建立在通信媒体基础上，实现设备之间的物理接口。

ISO 对 OSI 参考模型中的物理层做如下定义：

物理层为建立、维持与拆除数据链路实体之间二进制位流传输的物理连接，提供机械的、电气的、功能的和规程的特性。物理连接可以通过中继系统，允许进行全双工或半双工的二进制位流的传输。物理层的数据服务单元是比特，它可以通过同步或异步的方式进行传输。

1．物理层主要功能

计算机网络是由许多物理设备和传输介质构成的。但是，物理层并不是指这些物理设备或传输介质，而是有关物理设备通过物理传输介质进行互连的描述和规定。物理层要尽可能地屏蔽掉各种物理传输介质和通信手段的差异，使数据链路层感觉不到这些差异的存在。这样，数据链路层就不必考虑具体的传输介质，专心致力于完成本层的协议和服务。

物理层的作用就是在一条物理传输介质上，实现数据链路实体之间各种数据比特流的透明传输。因此，物理层应具有以下功能。

1）物理连接的建立、维持和释放

当两个数据链路实体之间请求建立连接时，物理层应能立即在它们之间建立相应的物理连接，这个连接可能要经过多个中继链路实体。在进行通信时，要维持这个连接。通信结束，物理层将立即释放这个连接。这里建立或激活有关连接的含义是：当发送端发送有关比特时，在这条链路的接收端要做好接收该比特的必要准备。

激活有关连接的过程就是要准备好一切必要的资源供收、发时使用。释放或激活一个连接，则是释放掉所使用的资源，为其他连接使用。

2）物理服务数据单元的传输

在物理层中使用的数据单元称为物理服务数据单元。在物理连接上，一般都是串行传输，即一比特一比特地按时间顺序传输，但有时也采用并行传输，即几比特同时传输。对于远距离的传输，通常都是串行的，只有近距离传输才采用并行的。物理层要提供这两类物理服务数据单元的传输，而且还要保证传输的顺序化。串行传输的方式可采用同步传输方式，也可采用异步传输方式。当采用同步传输方式时，系统要有同步功能进行收、发的同步；当采用异步传输方式时，系统则应配置异步适配器来完成数据的发送和接收功能。

3）物理层管理

物理层管理是指完成物理层的某些管理事务，如发送和接收的控制、异常情况的处理、故障情况的报告等。

2．物理层协议

物理层协议规定了与建立、维持与拆除物理信道有关的一些特性。这些特性分别是：机械特性、电气特性、功能特性和规程特性。

1）机械特性

机械特性是指实体间硬件连接接口的特性，它主要考虑：接口的形状、大小，接口引脚的个数、功能、规格，引脚的分布，相应通信媒体的参数和特性等。

2）电气特性

电气特性规定了在物理层传输的二进制比特流信号电平的高低、阻抗匹配、传输速

率和传输距离等。

3）功能特性

功能特性主要反映了接口电路的功能，即物理接口各条信号线的用途。

功能特性标准主要包括接口线功能规定方法和接口线功能分类两方面的内容。

4）规程特性

规程特性反映了利用接口进行传输位流的全过程及事件发生的可能顺序，它涉及到信号传输方式。

在物理层最常用的两种物理层标准是：EIA-232-E 接口标准和 RS-449 接口标准。

1.3.6　覆盖网与对等网

目前大多数网络上的应用都是基于传统的客户机/服务器模式（Client/Server，C/S）：服务器专门提供某种服务，用户通过客户机访问服务器来获得服务，例如收发邮件、浏览网页等。C/S 模式使得网络上的资源向服务器端集中，用户的通信高度依赖于服务器，用户之间无法直接交流信息。对等网（P2P 网、P2P 覆盖网）则是基于对等架构的工作模式。客户机/服务器模式与 P2P 模式的结构如图 1-44 所示。

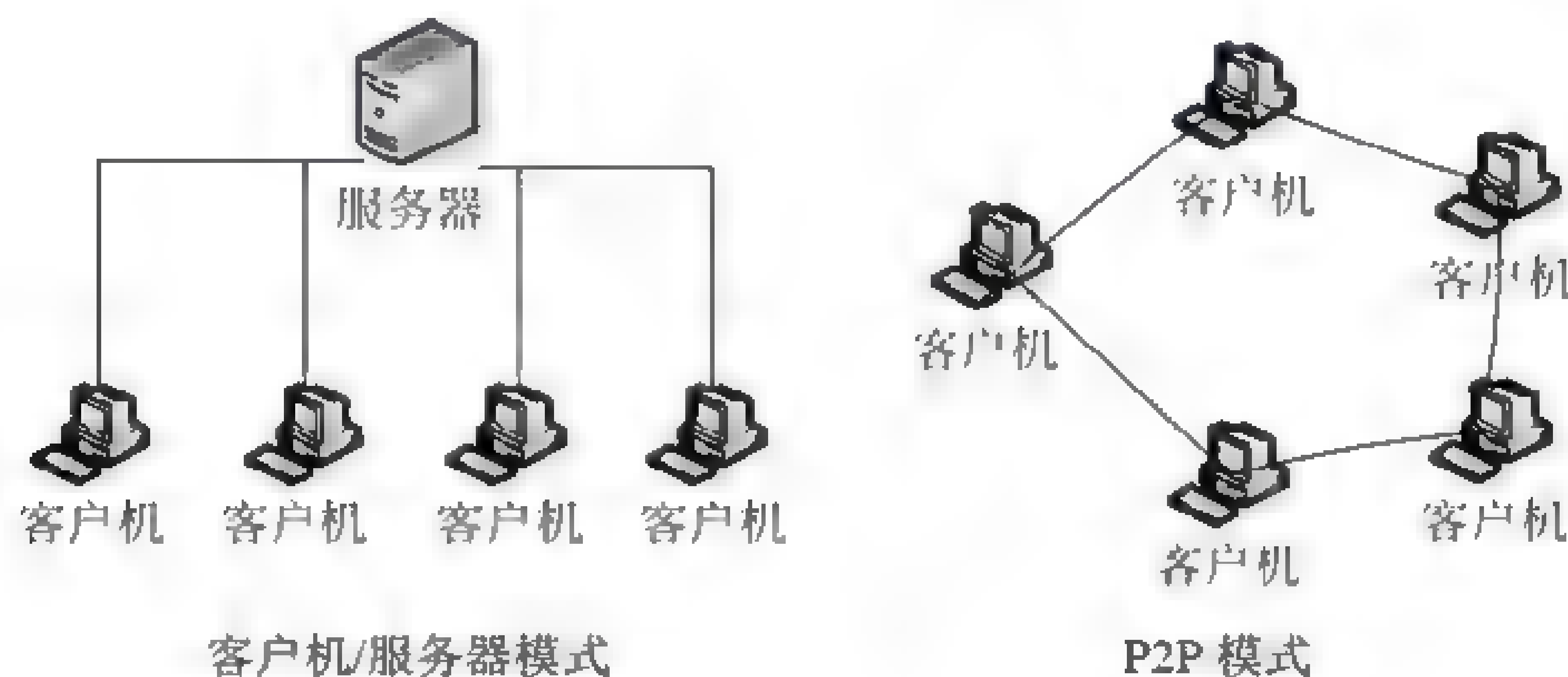


图 1-44　客户机/服务器模式与 P2P 模式

P2P 是 Peer-to-Peer 的缩写。P2P 网中所有参与系统的节点处于完全对等的地位，也可以理解为在覆盖网络中的每一个节点都同时扮演传统的 C/S 结构中的服务器和客户端角色，在向其他节点提供服务的同时，也接受来自其他节点的服务。因而，P2P 具有如下一些特性：

（1）peer 知道彼此的存在和位置。

（2）peer 既可以作为 Client 而存在，也可以作为 Server 而存在。

（3）多个 peer 可以形成一个 peer 组，并进而形成覆盖网。

（4）peer 都运行在这个虚拟的覆盖网上。

P2P 的这些特性使得 P2P 与 C/S 模式相比，可以大大改善资源的流量分布，解决网

络拥塞和带宽的瓶颈问题，减缓存储服务器的响应压力。

P2P 网主要完成：① 寻找到网络上其他的节点；② 发现一个节点提供何种服务；③ 从一个节点获取状态信息；④ 触发一个节点的一个服务；⑤ 创建、加入或离开覆盖网；⑥ 创建节点间的数据连接；⑦ 实施到其他节点的路由。

当前有很多种 P2P 网络并且每种 P2P 网络有着不同的特性，根据对象请求机制和 P2P 逻辑拓扑的不同，当前 P2P 体系结构可以分为三种。

（1）集中式 P2P 网络。

所有对象（peer）的索引保存在一台集中的服务器上。每个新加入的节点需要通知服务器它所保存的对象信息，以后其他节点只需要从服务器查询它所要对象所在节点的地址。这种 P2P 结构简单易部署。尽管有多个并行服务器，但它有单节点失效的问题。

（2）非集中式非结构化 P2P 网络。

对象请求是分布的，逻辑 P2P 拓扑通常是随机的无结构网络。请求一步一步地在网络中执行直到请求成功、失败或超时。没有单点失效，但是请求效率可能很低。

（3）分布式结构化 P2P 网络。

对象请求也是分布的，并且 P2P 的逻辑拓扑是某种结构的拓扑，如网状（mesh）、环状（ring）、d 维圆环面（d-dimension torus）和蝴蝶状（butterfly）等。这些结构化的拓扑通常用分布式哈希表（Distributed Hashing Table，DHT）构建。对象请求也是在结构化拓扑上逐跳执行，在理想情况下，能保证在有限跳后执行成功。

根据时间顺序和目的，当前的 P2P 网络可分为三代。

（1）第一代：早期的 P2P 网络，以容易且快速部署为目的。这代网络简单，但其可展性差或请求效率低。

（2）第二代：第二代 P2P 网络常利用 DHT 技术来实现更好的扩展性和更高的请求效率，并提供负载平衡和确定性查询保证。尽管如此，弹性或容错性并不是很好，特别是在恶意攻击的情况下。

（3）第三代：新近提出的 P2P 网络在假设节点以一定的失效概率离开的前提下，目的在于提供高弹性。产生弹性的常用方法有：复制、扩展节点之间的连接数以及一些特别的结构化拓扑。第二代和第三代 P2P 网络通常是分布的结构化覆盖网络。

1.4 网络设备与网络软件

1.4.1 网卡

1．网卡的概念

网络接口卡（Network Interface Card，NIC）又称网络适配器（Network Interface

Adapter，NIA），简称网卡。用于实现联网计算机和网络电缆之间的物理连接，为计算机之间相互通信提供一条物理通道，并通过这条通道进行高速数据传输。无论是双绞线连接、同轴电缆连接还是光纤连接，都必须借助于网卡才能实现数据的通信。在局域网中，每一台联网计算机都需要安装一块或多块网卡，通过介质连接器将计算机接入网络电缆系统。

2．网卡的组成

以最常见的 PCI 接口的网卡为例，一块网卡主要由 PCB 线路板、主芯片、数据汞、金手指（总线插槽接口）、BOOTROM、EEPROM、晶振、RJ-45 接口、指示灯、固定片等等，以及一些二极管、电阻电容等组成。如图 1-45 所示，展示了一个 PCI 网卡的解剖图。

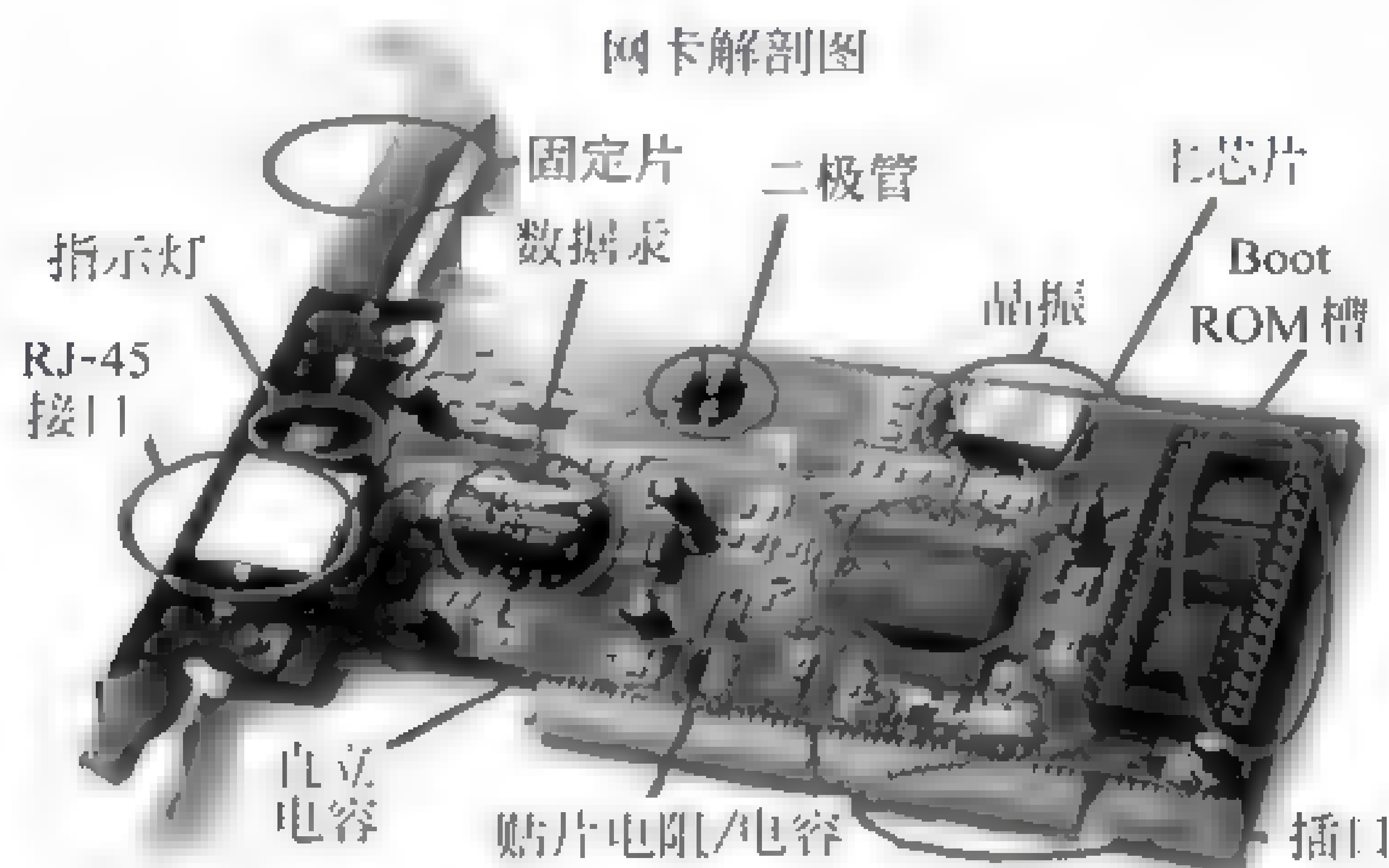


图 1-45　PCI 网卡的解剖图

3．网卡的功能

网卡完成物理层和数据链路层的大部分功能，包括网卡与网络电缆的物理连接、介质访问控制（如 CSMA/CD）、数据帧的拆装、帧的发送与接收、错误校验、数据信号的编/解码（如曼彻斯特代码的转换）、数据的串、并行转换等功能。网卡就像一个装卸货的小码头，负责计算机和网线之间的数据收发工作。

对于网卡而言，每块网卡都有一个唯一的地址，通常称为 MAC 地址或物理地址，是网卡在生产时由厂家烧入 ROM 中的。

1.4.2　交换机

在计算机网络系统中，“交换”是在对共享工作模式改进的基础上提出的。交换机也叫多端口网桥，工作在数据链路层，能够识别帧的内容。

1．交换机的内部结构

交换机拥有一条很高带宽的背部总线和内部交换矩阵。交换机在同一时刻可进行多

个端口对之间的数据传输。每一端口都可视为独立的网段，连接在其上的网络设备独自享有全部的带宽，无须同其他设备竞争使用。其内部结构如图 1-46 所示。

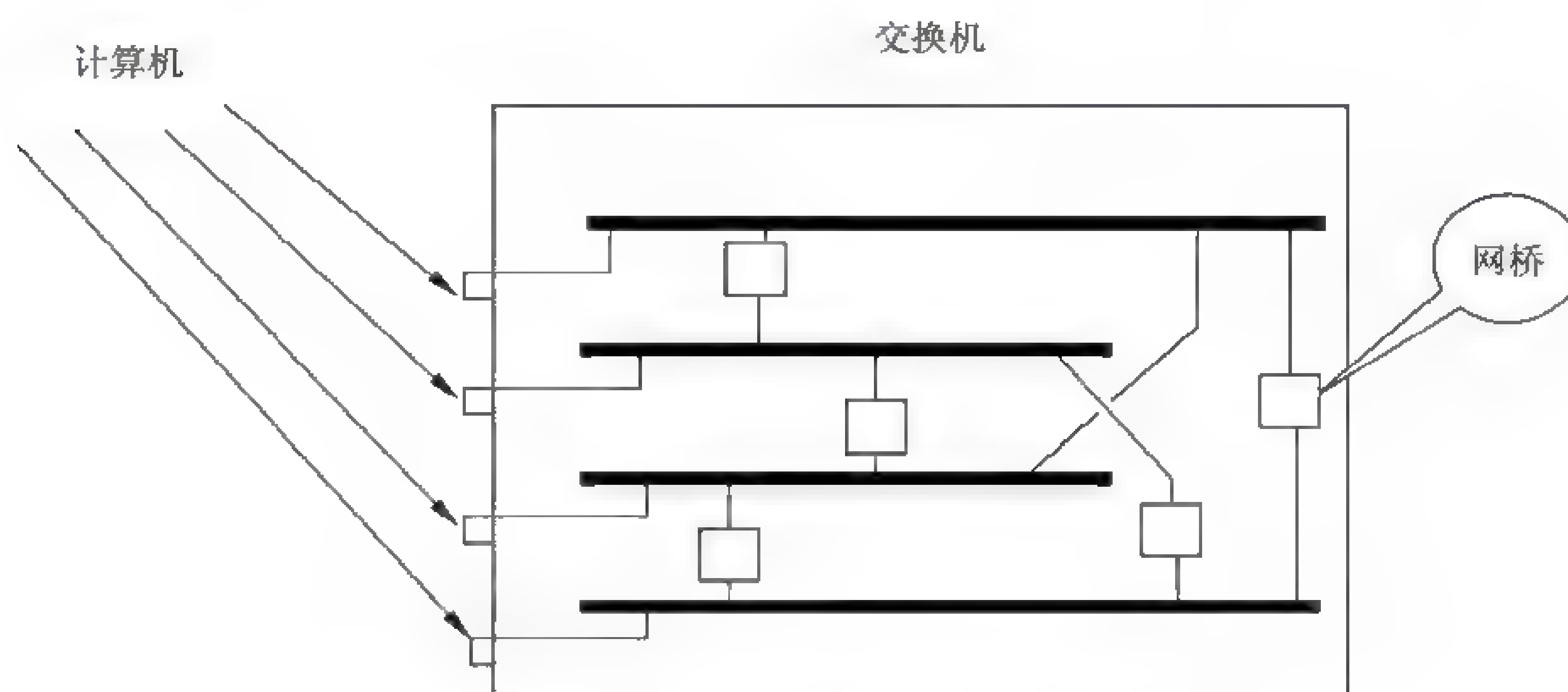


图 1-46 交换机（多端口网桥）的内部结构

2. 交换机的功能

交换机主要有以下三个功能。

- 学习：交换机对每一端口相连设备的 MAC 地址进行识别，并将这些设备的 MAC 地址同相应端口的映射关系存放在自己缓存中的 MAC 地址表中。
- 转发/过滤：当一个数据帧的目的地址在 MAC 地址表中有映射关系存在时，它被转发到响应的端口而不是所有端口（如该数据帧为广播/组播帧则转发至所有端口）。
- 消除回路：当交换机包括一个冗余回路时，交换机通过生成树协议避免回路的产生，同时允许存在后备路径。

使用交换机也可以把网络“分段”，通过对照地址表，交换机只允许必要的网络流量通过交换机。通过交换机的过滤和转发，可以有效的隔离广播风暴，减少误包和错包的出现，避免共享冲突。

3. 交换机的工作原理

交换机是依赖于一张 MAC 地址与端口的映射表（Context Address Map，CAM）来进行工作的，如图 1-47 所示。

交换机是一种基于 MAC 地址识别，能完成封装转发数据帧功能的网络设备。交换机可以“学习”MAC 地址，并把其存放在内部地址表中，通过在数据帧的始发者和目标接收者之间建立临时的交换路径，使数据帧直接由源地址到达目的地址。

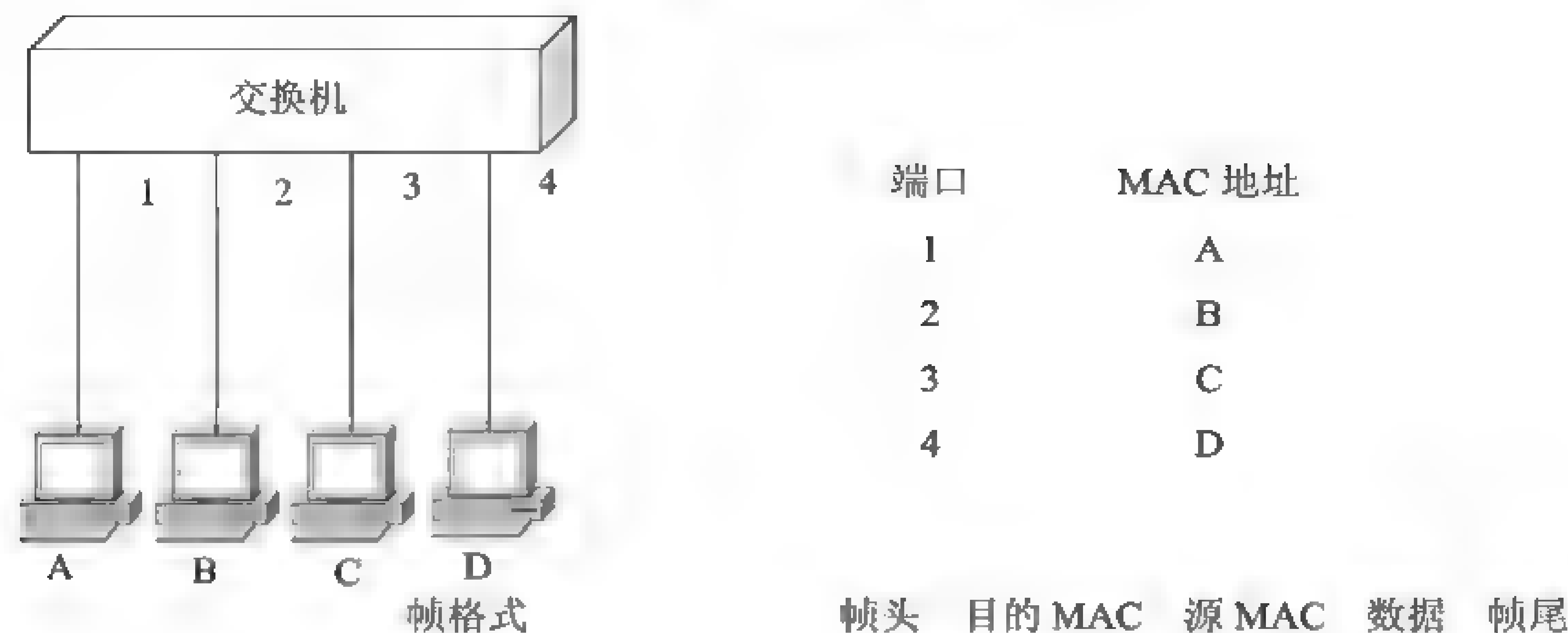


图 1-47　交换机工作原理

如图 1-47 所示，数据帧中包含了目的 MAC 和源 MAC，源 MAC 就是发送数据帧的计算机的网卡地址，目的 MAC 就是接收数据帧的计算机的网卡地址。交换机刚开机时，这张 MAC 地址与端口的映射表是空的；但计算机 A 想发送数据给 B 时，数据帧的目的 MAC 为 B 的 MAC，源 MAC 为 A 的 MAC，交换机并不知道 B 是接在哪个端口上，所以数据会从 2，3，4，发送出去以保证计算机 B 能够接收到；然而由于交换机是从端口 1 收到 A 发送的数据，即在帧中的源 MAC 是 A 的 MAC 地址，所以交换机就把 A 的 MAC 记录在端口 1 上；但其他计算机（例如计算机 B）要发送数据给 A 时，数据帧的目的 MAC 为 A 的 MAC，源 MAC 为 B 的 MAC，交换机已经知道 A 的 MAC 在端口 1 了，所以这时数据只会从端口 1 发送出去，而不会从端口 3，4 发送出去；同时由于交换机是从端口 2 收到 B 发送的数据，交换机也会往表中添加一条记录，指明 B 的 MAC 在端口 2 上，下次计算机 A 发送给 B 时，数据只会从端口 2 发送出去了，而不是像以前一样从其他所有的端口发送出去。

交换机的工作原理：交换机根据收到数据帧中的源 MAC 地址建立该地址同交换机端口的映射关系并将其写入 MAC 地址表中。当一台计算机发送过一次数据帧时，就被交换机记录下来；如果有其他的计算机向这台计算机发送数据时，数据只会从特定端口转发出去，而不会从其他端口转发。如果交换机收到的数据帧中的目的 MAC 地址不在 MAC 地址表中，则向所有端口转发。另外，广播帧和组播帧也向所有的端口转发。

从以上的分析可知，如果交换机已经完成了 MAC 地址与端口映射表的建立，计算机 A 发送数据给 B 时，端口 3，4 并无数据存在，这就意味着计算机 C 可以同时发送数据给 D。A 和 C 不会因为同时发送数据而产生冲突，即它们不在同一冲突域。 这一点和集线器有着很大的不同，交换机所连接的计算机可以独占端口的带宽。交换机的这个特性可以概括为：交换机可以隔离冲突域，交换机的每个端口就是一个小的冲突域。

交换机能够分析计算机所发送的数据帧中包含的源 MAC（即发送者）和目的 MAC（即接收者），并用来建立和更新映射表。交换机中 MAC 地址与端口的映射表中的记录

实际上有一定的时效性，通常为 300s，如果一条记录在 300s 内没有得到更新，记录就会被删除。这样的好处是防止 CAM 表被迅速占满，同时也是为了使得计算机从一个端口移动到另一端口上后还可以正常工作。

当交换机收到目的 MAC 为 0XFFFFFFFFFFFF（广播地址）的数据帧时，它会把该数据从所有端口转发出去，也就是说交换机不能隔离广播域。因此如果网络中的计算机数量较多，只要有一台计算机发出广播，网络中就会充斥着大量的广播包，从而影响正常的数据帧的传输。因此，大型的网络仅仅采用交换机来构建也是不合适的。

4. 第二层交换与第三层交换

1）第二层交换

第二层交换是以硬件的方式执行网桥的功能。上述内容涉及的都是第二层交换技术。

2）第三层交换

第三层交换是将路由功能集成到交换机中，在交换机内部实现了路由，提高了网络的整体性能。但它并不是简单的把路由器设备的硬件及软件简单地叠加在局域网交换机上。简单地说，三层交换技术就是：二层交换技术＋三层转发技术。

三层交换机在对第一个数据流进行路由后，会产生一个 MAC 地址与 IP 地址的映射表，当同样的数据流再次通过时，将根据此表直接从二层交换而不是再次路由，提供线速性能，从而消除了路由器进行路由选择而造成网络的延迟，提高了数据包转发的效率，消除了路由器可能产生的网络瓶颈问题。

5. 交换机的类型

根据网络覆盖范围划分：局域网交换机和广域网交换机。

根据传输介质和传输速度划分：以太网交换机、快速以太网交换机、千兆以太网交换机、10 千兆以太网交换机、ATM 交换机、FDDI 交换机和令牌环交换机。

根据交换机应用网络层次划分：企业级交换机、校园网交换机、部门级交换机和工作组交换机、桌机型交换机。

根据交换机端口结构划分：固定端口交换机和模块化交换机。

根据工作协议层划分：第二层交换机、第三层交换机和第四层交换机。

根据是否支持网管功能划分：网管型交换机和非网管型交换机。

6. 交换机堆叠与级联

堆叠（stack）和级联（uplink）是多台交换机或集线器连接在一起的两种方式。它们的主要目的是增加端口密度。但它们的实现方法是不同的。简单地说，级联可通过一根双绞线在任何网络设备厂家的交换机之间，集线器之间，或交换机与集线器之间完成。而堆叠只有在自己厂家的设备之间，且此设备必须具有堆叠功能才可实现。级联只需单做一根双绞线（或其他媒介），堆叠需要专用的堆叠模块和堆叠线缆，而这些设备可能需要单独购买。交换机的级联在理论上是没有级联个数限制的（注意：集线器级联有个数

限制，且 10M 和 100M 的要求不同)，而堆叠各个厂家的设备会标明最大堆叠个数。以下分别介绍其实现原理及详细连接过程。

1）交换机堆叠

此种连接方式主要应用在大型网络中对端口需求比较大的情况下使用。交换机的堆叠是扩展端口最快捷、最便利的方式，同时堆叠后的带宽是单一交换机端口速率的几十倍。但是，并不是所有的交换机都支持堆叠的，这取决于交换机的品牌、型号是否支持堆叠；并且还需要使用专门的堆叠电缆和堆叠模块；最后还要注意同一堆叠中的交换机必须是同一品牌。

堆叠主要通过厂家提供的一条专用连接电缆，从一台交换机的 UP 堆叠端口直接连接到另一台交换机的 DOWN 堆叠端口。堆叠中的所有交换机可视为一个整体的交换机来进行管理。

堆叠的优点是不会产生性能瓶颈，因为通过堆叠，可以增加交换机的背板带宽，不会产生性能瓶颈。通过堆叠可以在网络中提供高密度的集中网络端口，根据设备的不同，一般情况下最大可以支持 8 层堆叠，这样就可以在某一位置提供上百个端口。堆叠后的设备在网络管理过程中就变成了一个网络设备，只要赋予一个IP 地址，方便管理，也节约管理成本。堆叠的缺点主要是受设备限制，并不是所有的交换机都支持堆叠的，不同厂家，不同型号，进行堆叠需要特定的设备的支持。受距离限制，因为受到堆叠线缆长度的限制，堆叠的交换机之间的距离要求很近。还有就是不同厂家的设备有时不能很好的兼容，因此不同厂家的设备想要进行堆叠非常困难。

2）交换机级联

级联是最常见的连接方式，就是使用网线将两个交换机进行连接。连接的结果是，在实际的网络中，它们仍然各自工作，仍然是两个独立的交换机。需要注意的是交换机不能无限制级联，超过一定数量的交换机进行级联，最终会引起广播风暴，导致网络性能严重下降。级联又分为以下两种：

（1）使用普通端口级联。

所谓普通端口就是通过交换机的某一个常用端口（如 RJ-45 端口）进行连接。需要注意的是，这时所用的连接双绞线要用反线，即是说双绞线的两端要跳线（第 1-3 与 2-6 线脚对调）。

（2）使用 Uplink 端口级联。

在所有交换机端口中，都会在旁边包含一个 Uplink 端口。此端口是专门为上行连接提供的，只需通过直通双绞线将该端口连接至其他交换机上除“Uplink 端口”外的任意端口即可（注意，并不是 Uplink 端口的相互连接)。

级联的优点是可以延长网络的距离，理论上可以通过双绞线和多级的级联方式无限远的延长网络距离，级联后，在网络管理过程中仍然是多个不同的网络设备。另外级联基本上不受设备的限制，不同厂家的设备可以任意级联。级联的缺点就是多个设备的级

联会产生级联瓶颈。例如，两个百兆交换机通过一根双绞线级联，这时它们的级联带宽是百兆，这样不同交换机之间的计算机要通信，都只能通过这百兆带宽。

综合以上两种方式来看，交换机的级联方式实现简单，只需一根普通的双绞线即可，节约成本而且基本不受距离的限制；而堆叠方式投资相对较大，且只能在很短的距离内连接，实现起来比较困难。

但也要认识到，堆叠方式比级联方式具有更好的性能，信号不易衰竭，且通过堆叠方式，可以集中管理多台交换机，大大简化了管理工作量；如果实在需要采用级联，也最好选用 Uplink 端口的连接方式。因为这可以在最大程度上保证信号强度，如果是普通端口之间的连接，必定会使网络信号严重受损。

1.4.3 路由器

1．路由器有关概念

路由器是属于网络层的互联设备，用于连接多个逻辑上分开的网络，所谓逻辑网络就是拥有独立网络地址的网络。

2．路由器的构成

路由器的构成如图 1-48 所示。

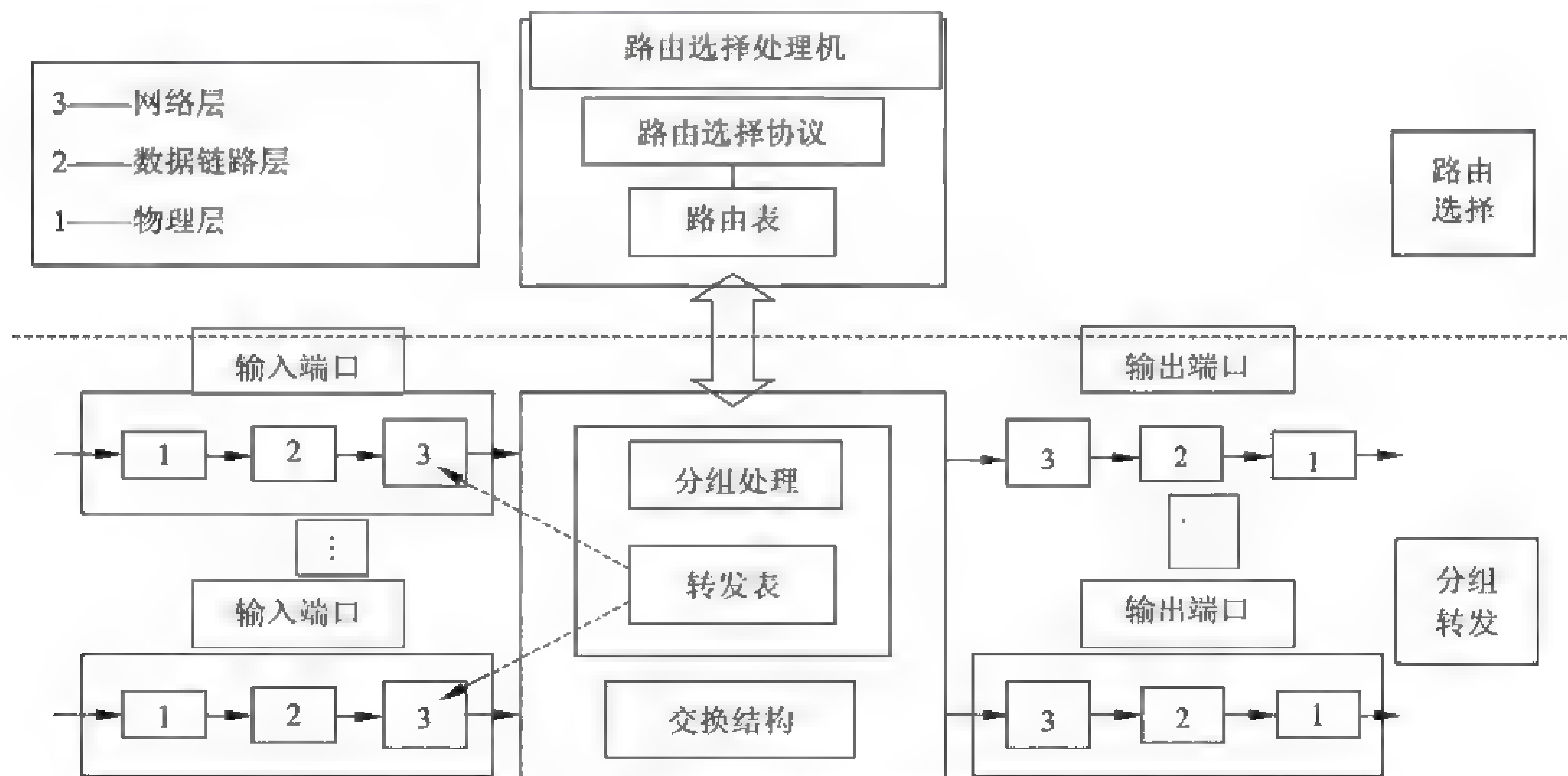


图 1-48 路由器的组成

3．路由器的功能

路由器主要有以下几种功能。

- 网络互连：路由器支持各种局域网和广域网接口，主要用于互连局域网和广域网。

- 路由选择：通过路由器互连在一起的网络，如果一个网络中的主机要向另一个网络的主机发送数据包，路由器就会分析源地址和目的节点地址中的网络号，找出一条最佳的、最经济、最快捷的一条通信路径。
- 分组转发：接收节点发来的数据包，然后根据数据包中的源地址和目的地址，对照自己缓存中的路由表，把数据包直接转发到目的节点。
- 拆分和包装数据包：路由器在转发数据包的过程中，由于网络带宽等因素，按照预定的规则把大的数据包分解成适当大小的数据包，到达目的地后再把分解的数据包包装成原有形式。
- 拥塞控制：为了保证整个网络的传输效率，路由器防止过多的数据注入网络。
- 网络管理：路由器提供包括配置管理、性能管理、容错管理和流量控制等功能。

另外路由器还有网络计费的功能。

4. 路由器工作原理

图 1-49 中局域网 1 中的源节点 101 生成了一个或多个分组，这些分组带有源 IP 地址与目的 IP 地址。如果局域网 1 中的 101 节点要向局域网 3 中的目的节点 104 发送数据，那么它只需按正常工作方式将带有源 IP 地址与目的 IP 地址分组装配成帧发送出去。连接在局域网 1 的路由器接收到来自源节点 101 的帧后，由路由器的网络层检查分组头，根据分组的目的 IP 地址去查路由表，确定该分组输出路径。路由器确定该分组的目的节点在局域网 3，它会将该分组发送到目的节点所在的局域网。

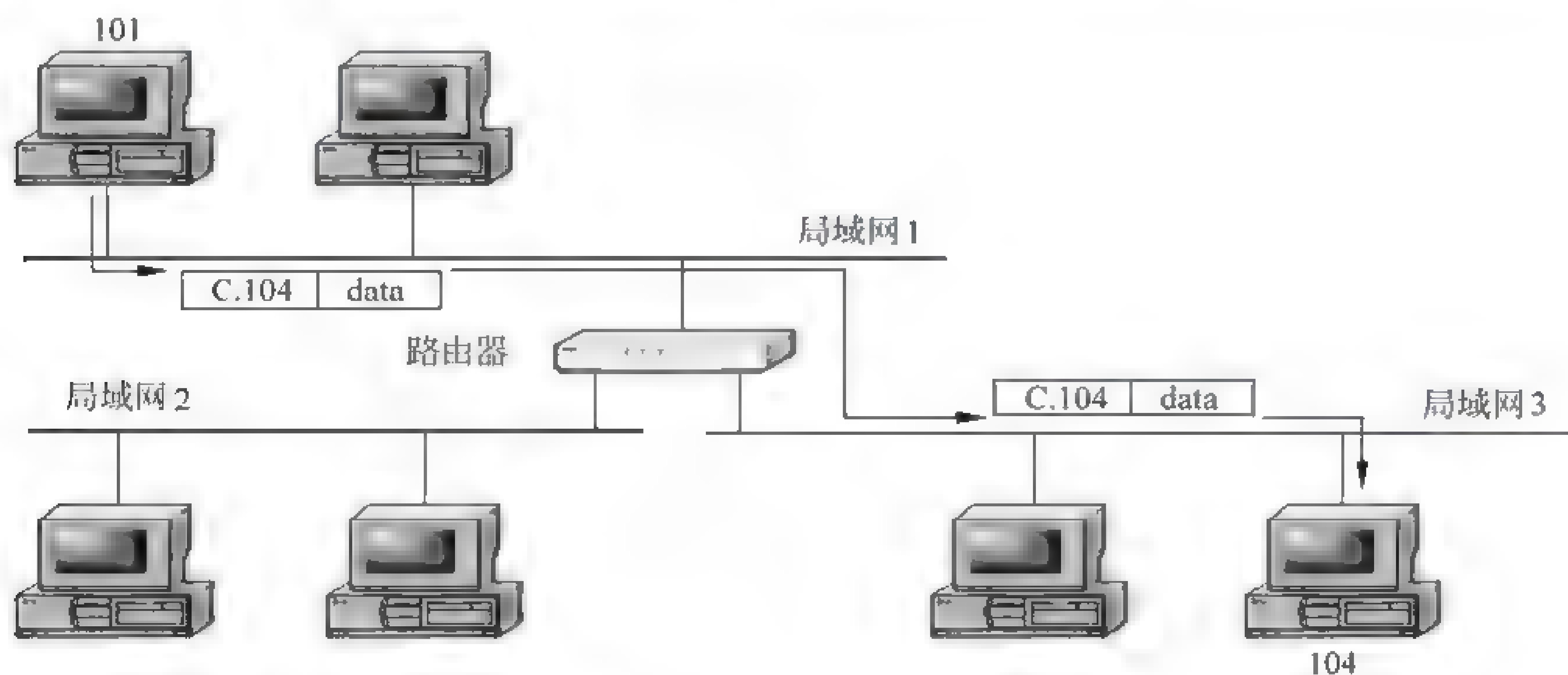


图 1-49　路由器工作原理

一般来说，路由器的主要工作是对数据包进行存储转发，具体过程如下。

第一步，当数据包到达路由器，根据网络物理接口的类型，路由器调用相应的链路层功能模块，以解释处理此数据包的链路层协议报头。这一步处理比较简单，主要是对

数据的完整性进行验证，如 CRC 校验、帧长度检查等。

第二步，在链路层完成对数据帧的完整性验证后，路由器开始处理此数据帧的 IP 层。这一过程是路由器功能的核心。根据数据帧中 IP 包头的目的 IP 地址，路由器在路由表中查找下一跳的 IP 地址；同时，IP 数据包头的 TTL（time to live）域开始减数，并重新计算校验和（checksum）。

第二步，根据路由表中所查到的下一跳 IP 地址，将 IP 数据包送往相应的输出链路层，被封装上相应的链路层包头，最后经输出网络物理接口发送出去。

简单地说，路由器的主要工作就是为经过路由器的每个数据包寻找一条最佳传输路径，并将该数据包有效地传送到目的站点。由此可见，选择最佳路径策略或叫选择最佳路由算法是路由器的关键所在。为了完成这项工作，在路由器中保存着各种传输路径的相关数据——路由表（routing table），供路由选择时使用。上述过程描述了路由器的主要而且关键的工作过程，但没有说明其他附加性能，例如访问控制、网络地址转换、排队优先级等。

1.4.4 网关

1. 网关的概念

网关又叫协议转换器，是一种复杂的网络连接设备，可以支持不同协议之间的转换，实现不同协议网络之间的互连。网关具有对不兼容的高层协议进行转换的能力，为了实现异构设备之间的通信，网关需要对不同的链路层、专用会话层、表示层和应用层协议进行翻译和转换。

网关主要用于不同体系结构的网络或者局域网与主机系统的连接。在互连设备中，它最为复杂，一般只能进行一对一的转换，或是少数几种特定应用协议的转换。网关一般是一种软件产品。目前，网关已成为网络上每个用户都能访问大型主机的通用工具。

2. 网关的分类

网关的分类主要有三种：协议网关 、应用网关、安全网关。

- 协议网关：协议网关通常在使用不同协议的网络区域间做协议转换。
- 应用网关：应用网关是在使用不同数据格式间翻译数据的系统。
- 安全网关：安全网关是各种技术的融合，具有重要且独特的保护作用，其范围从协议级过滤到十分复杂的应用级过滤。

1.4.5 无线接入点

无线接入点（Access Point，AP）是一个包含单纯性无线接入点（无线 AP）和无线路由器（含无线网关、无线网桥）等类设备的统称。

单纯性无线 AP 就是一个无线的交换机，仅仅是提供一个无线信号发射的功能。单

纯性无线 AP 的工作原理是将网络信号通过双绞线传送过来，经过 AP 产品的编译，将电信号转换成为无线电信号发送出来，形成无线网的覆盖。根据不同的功率，其可以实现不同程度、不同范围的网络覆盖，一般无线 AP 的最大覆盖距离可达300m。

多数单纯性无线 AP 本身不具备路由功能，目前大多数的无线 AP 都支持多用户（30～100 台计算机）接入、数据加密、多速率发送等功能，在家庭、办公室内，一个无线 AP 便可实现所有计算机的无线接入。

单纯性无线 AP 亦可对装有无线网卡的计算机做必要的控制和管理。单纯性无线 AP 既可以通过 10Base-T（WAN）端口与内置路由功能的ADSL MODEM或 CABLE MODEM（CM）直接相连，也可以在使用时通过交换机/集线器、宽带路由器再接入有线网络。

无线 AP 跟无线路由器类似，按照协议标准本身来说 IEEE 802.11b 和 IEEE 802.11g 的覆盖范围是室内 100m、室外300m。这个数值仅是理论值，在实际应用中，会碰到各种障碍物，其中以玻璃、木板、石膏墙对无线信号的影响最小，而混凝土墙壁和铁对无线信号的屏蔽最大。所以通常实际使用范围是：室内 30m、室外 100m（没有障碍物）。

作为无线网络中重要的环节无线接入点、无线网关也就是无线 AP，它的作用其实就类似于我们常用的有线网络中的集线器。在那些需要大量 AP 来进行大面积覆盖的公司使用得比较多，所有 AP 通过以太网连接起来并连到独立的无线局域网防火墙。但同时由于其一般专用无线 AP 都不带额外的局域网接口，使其应用范围较窄。

1.4.6　调制解调器

调制解调器（modem），是计算机与电话线之间进行信号转换的装置。通过调制解调器和电话线就可以实现计算机之间的数据通信。 目前调制解调器主要有两种：内置式和外置式。

内置式调制解调器其实就是一块计算机的扩展卡，插入计算机内的一个扩展槽即可使用，它无须占用计算机的串行端口。它的连线相当简单，把电话线接头插入卡上的 Line 插口，卡上另一个接口 Phone 则与电话机相连，平时不用调制解调器时，电话机使用一点也不受影响。

外置式调制解调器则是一个放在计算机外部的盒式装置，它需占用计算机的一个串行端口，还需要连接单独的电源才能工作，外置式调制解调器面板上有几盏状态指示灯，可方便监视 Modem 的通信状态，并且外置式调制解调器安装和拆卸容易，设置和维修也很方便，还便于携带。外置式调制解调器的连接也很方便，phone 和 line 的接法同内置式调制解调器。但是外置式调制解调器得用一根串行电缆把计算机的一个串行口和调制解调器串行口连起来，这根串行线一般随外置式调制解调器配送。

调制解调器的一个重要性能参数是传输速率，目前市面上 28.8K、33.6K 和 56K 的调制解调器都有，而且 56K 的调制解调器已经成为市场的主流产品。但由于国内通信线

路的限制，以及用户太多、国际出口太少的缘故，平时使用很难达到上述速率，因此，如果使用时传输速率显示只有每秒几 K 甚至更低，也不用怀疑计算机或调制解调器有什么问题。

1.4.7 网络软件

网络软件包括通信支撑平台软件、网络服务支撑平台软件、网络应用支撑平台软件、网络应用系统、网络管理系统以及用于特殊网络站点的软件等。从网络体系结构模型不难看出，通信软件和各层网络协议软件是这些网络软件的基础和主体。

1）通信软件

通信软件用以监督和控制通信工作的软件。它除了作为计算机网络软件的基础组成部分外，还可用作计算机与自带终端或附属计算机之间实现通信的软件。通信软件通常由线路缓冲区管理程序、线路控制程序以及报文管理程序组成。报文管理程序通常由接收、发送、收发记录、差错控制、开始和结束 5 个部分组成。

2）网络协议软件

网络协议软件是网络软件的重要组成部分。按网络所采用的协议层次模型(如 ISO 建议的开放系统互连基本参考模型）组织而成。除物理层外，其余各层协议大都由软件实现。每层协议软件通常由一个或多个进程组成，其主要任务是完成相应层协议所规定的功能，以及与上、下层的接口功能。

3）网络应用系统

网络应用系统是根据网络的组建目的和业务的发展情况，研制、开发或购置。其任务是实现网络总体规划所规定的各项业务，提供网络服务和资源共享。网络应用系统有通用和专用之分。通用网络应用系统适用于较广泛的领域和行业，如数据收集系统、数据转发系统和数据库查询系统等。专用网络应用系统只适用于特定的行业和领域，如银行核算、铁路控制、军事指挥等。一个真正实用的、具有较大效益的计算机网络，除了配置上述各种软件外，通常还应在网络协议软件与网络应用系统之间，建立一个完善的网络应用支撑平台，为网络用户创造一个良好的运行环境和开发环境。功能较强的计算机网络通常还设立一些负责全网运行工作的特殊主机系统（如网络管理中心、控制中心、信息中心、测量中心等）。对于这些特殊的主机系统，除了配置各种基本的网络软件外，还要根据它们所承担的网络管理工作编制有关的特殊网络软件。

在计算机网络软件方面受到重视的研究方向有：全网界面一致的网络操作系统，不同类型计算机网络的互连（包括远程网与远程网、远程网与局域网、局域网与局域网），网络协议标准化及其实现，协议工程（协议形式描述、一致性测试、自动生成等），网络应用体系结构和网络应用支撑技术研究等。

1.5　局域网

1.5.1　局域网概述

1．局域网定义

局域网为计算机局部区域网络（LAN）的简称。IEEE 局域网络标准委员会对局域网的描述性定义为：局域网是一种为单一机构所拥有的专用计算机网络，其通信被限制在中等规模的地理范围，如一栋办公楼、一座工厂或一所学校，具有较高数据速率和较低的误码率，能有效实现多种设备之间互联、信息交换和资源共享。

局域网的特征如下。

- 范围小：通常在 2.5km 以内。
- 高数据率：10Mbps 以上，现在已达到 10Gbps。
- 低误码率：一般可达到 10^{-9} 以下。
- 单一部门所有。
- 支持实时应用。

2．局域网拓扑结构

局域网的主要拓扑结构有总线型、环型和星型。

总线型局域网是将计算机以总线连接起来构成的局域网，是最早的局域网，采用同轴电缆作为传输介质，使用 CSMA/CD 访问控制方式控制对总线的访问。当使用细同轴电缆时，总线长度不超过 300m，工程上一般不超过 185m，可连接的节点数不超过 30 个。可借助中继器将最多 5 段总线连接在一起，组成更大的局域网。当使用粗同轴电缆时，总线长度不超过 500m，可连接的节点数不超过 100 个。可借助中继器将最多 5 段总线连接在一起，组成可延伸至 2.5km 的局域网。总线型局域网现在已经被淘汰。

环型局域网利用环接口设备将传输介质连接成环状，计算机连接到环接口设备上。所组成的环可以是单环，也可以是双环。信号在环上一定是单向传送的。环型局域网现在已基本上不再使用，但环型广域网（如 SDH 网络）还在广泛使用。

星型局域网将计算机连接到中央计算机或连接设备形成的局域网，是目前广泛使用的局域网。早期使用集线器（hub）将计算机连接起来组成星型拓扑，但仍然使用 CSMA/CD 访问控制方式，集线器相当于一条逻辑总线。这种使用物理上星型、逻辑上总线的局域网的显著优点是可维护性显著改善，其中一台计算机或一条电缆或一个网卡的故障，不会影响其他计算机的正常连网。

局域网交换机的出现，大大提高了星型网的性能，也迅速取代了传统的集线器。

3. 以太网

Bob Metcalfe 对以太网的产生作出了重大的贡献，被称为以太网之父。

1972 年 Bob Metcalfe 在 Xerox 公司的 PARC 计算机实验室工作时，主要研究任务是如何将他们的第一台个人计算机 Alto 和第一台激光打印机 EARS 互联起来。1972 年底 Metcalfe 和同事 David Boggs 开发出第一个实验性的局域网系统，实验系统的数据传输率达到 2.94Mbps。

1973 年 5 月 22 日，Metcalfe 与 Boggs 在 Alto Ethernet 中提出了以太网工作原理设计方案。他们受到 19 世纪物理学家解释光在空间中传播的介质“以太（ether）”的影响，将这种局域网命名为 Ethernet（以太网），寓意无所不在的网络。

Ethernet 的核心技术是共享总线的介质访问控制方法 CSMA/CD（带冲突检测的载波侦听多路访问），用于解决多个节点共享总线的发送权问题。

1977 年 Metcalfe 申请了相关专利。

1980 年，Xerox、Intel、DEC 公司合作，制定了以太网物理层、数据链路层规范，命名为 DIX 规范。该规范规定，以太网为总线拓扑结构，使用同轴电缆作为传输介质，使用 CSMA/CD 访问控制方式，使用曼彻斯特编码，数据率为 10Mbps。1981 年 DIX 2.0 发布，1982 年 IEEE 802 委员会以 DIX2.0 为基础（几乎未作修改），发布了 IEEE 802.3 协议，成为现在以太网的通用标准。

1995 年 100Mbps 以太网标准发布，1998 年 1Gbps 以太网标准发布，2002 年，10Gbps 以太网标准发布。

1.5.2 访问控制方式

1.5.2.1 访问控制方式的分类

访问控制方式用于控制节点对介质的访问，解决两个问题：一是确定每个节点能把信息送到通信介质上去的特定时刻，二是确定如何有效利用共享通信介质。

按实现方式的不同，可以将访问控制方式分为以下三类。

- 不加控制：不进行任何控制，每个节点想发送信息就发送信息。一般而言，只有每个节点具有专用信道的网络才能使用此种方式。
- 集中控制：由中央节点负责分配发送权，只有获得发送权的节点才能发送数据。比如时间片方式、轮询方式等。
- 分布控制：没有中央控制节点，各节点采用分布协调方式分配发送权。比如令牌传递控制方式、CSMA/CD 方式等。

1.5.2.2 令牌传递访问控制方式

令牌传递访问控制方式要求网络满足的条件是：网络形成环，当不能形成物理环时，

必须形成逻辑环；信号在环上单向传输。

1．令牌传递访问控制方式原理

① 监控节点产生唯一一个令牌沿环路传输。

② 要发送数据的节点等待令牌。获得令牌后往令牌上附加数据帧，填写相应标志后让其继续传送。

③ 目的节点检测到数据帧后拷贝帧，设置应答标志后让其继续传送。

④ 数据帧回到源节点后，源节点根据应答标志确定撤销或重传。

⑤ 非源、非目的节点，转发帧。

在采用令牌传递控制方式的网络中，每个节点可能进行的操作有以下 4 种。

- 发送：源节点进行。
- 拷贝：目的节点进行。
- 转发：非源、非目的节点进行。
- 撤销：源节点进行。

2．令牌传递访问控制方式问题及对策

1）令牌丢失

一旦令牌丢失，则任何节点都无法获得令牌，所有节点都不能发送数据。因此，必须有防令牌丢失的措施。

判断令牌丢失的方法是：如果在给定的时间内，没有令牌经过本节点，则本节点可以判断令牌丢失，该时间可以根据环长计算出来。环型网一旦安装，其环的长度就确定了，令牌在其上传递一周的时间就可计算出来。当然，也可设定一个最大环长，据此计算令牌传递一周的时间。比如 FDDI 网络，规定最大环长为 200km。

通常，由监控节点监视令牌是否丢失。一旦发现令牌丢失，立即生成一个新令牌。

2）令牌增生

当网络上有多个令牌时，可能导致冲突发生。例如一个节点正在发送、转发或拷贝一个数据帧的过程中，又到达另一个帧，两个帧交叉在一起，导致帧被破坏。

判断令牌是否增生的方法是：如果一个节点持有令牌又收到令牌或数据帧，则可断定令牌增生。

解决令牌增生的方法很简单，只要丢弃一个令牌就行了。

3）地址错误

如果一个帧在传递过程中地址出错了，则会导致严重问题。如果源地址出错，则该帧将不会被撤销，这样其他节点就不能获得令牌发送数据。因此需要有防止地址出错的机制。通常，可由监控节点完成此项工作，其方法是在帧中设置一个特殊标志，源节点发送数据时设置为一个特殊值，当经过目的节点或源节点时，修改一次该值。监控节点如果监测到一个帧连续两次经过且标志未发生改变，就认为该帧是一个错误帧，将其撤销。

1.5.2.3 CSMA/CD 访问控制方式

载波侦听多路访问/冲突检测（CSMA/CD）控制方式早期要求网络组成总线拓扑结构，后来采用集线器和交换机的星型局域网络也继续使用该方式。

1．CSMA/CD 原理

CSMA/CD 的工作过程如下：

① 每个节点在发送数据前，先监听信道，以确定介质上是否有其他节点发送的信号在传送。

② 若介质忙（有信号在传送），则继续监听。

③ 否则，若介质处于空闲状态，则立即发送信息。

④ 在发送过程进行冲突检测。如果发生冲突，则立即停止发送，并向总线上发出一串阻塞信号（全 1）强化冲突，以保证总线上所有节点都知道冲突已发生，转⑤。

⑤ 随机延迟一段时间后返回①。

由于在发送过程中进行监听，保证在发送过程中没有出现冲突，源节点只要将帧正常发送完毕，就认为目的节点能正常接收到，因此该方法不需要发送应答帧。

2．延迟时间的确定

CSMA/CD 在检测到冲突后，随机延迟一段时间，该时间长度按截断的二进制直属退避算法确定。

假定信号在总线上往返传递的时间为 t（称为时间片），本帧在发送过程中已检测到的冲突次数是 n，则延迟的时间片数 T=0～2^k–1 之间的随机数，k=min{n,10}。一个帧在发送过程中经历的冲突次数越多，说明网络负载越重，k 就越大，相应地 T 就越大（概率意义上）。这是一种对负载具有自适应能力的方法。

k 最大取 10，限制最大延迟时间在一个给定范围。

1.5.3 局域网协议

1.5.3.1 IEEE 802 LAN 体系结构与协议

1980 年 2 月 IEEE 成立 IEEE 802 委员会，负责制定局域网标准。IEEE 802 委员会认为，局域网内没有路由选择、拥塞控制等问题，因此不需要网络层，高层可由用户去实现，因此局域网只有物理层和数据链路层。同时，将数据链路层分为与拓扑结构无关的逻辑链路控制子层（LLC 层）和与拓扑结构、访问控制方式相关的介质访问控制子层（MAC 层）。LLC 负责与应用接口，MAC 负责与介质接口。将物理层细分为物理信号子层 PS、连接接口子层 AUI、物理介质接入层 PMA 和介质相关接口 MDI 4 个子层。

IEEE 802 委员会制定一系列标准，主要包括。

- IEEE 802.1A：局域网概述及体系结构。

- IEEE 802.1B：寻址、网络互连与网络管理。
- IEEE 802.2：逻辑链路控制（LLC）。
- IEEE 802.3：以太网的 CSMA/CD 总线访问控制方法与物理层规范。
- IEEE 802.3i：10Base-T3 对 UTP 以太网规范。
- IEEE 802.3u：100Base-T 星型 UTP 以太网规范。
- IEEE 802.3z：1000Base-T UTP 以太网规范。
- IEEE 802.3z：1000Base-CX STP 以太网规范。
- IEEE 802.3z：1000Base-LX 光纤以太网规范。
- IEEE 802.3ae：10GBase 以太网规范。
- IEEE 802.4：令牌总线（Token Bus）访问控制方法与物理层规范。
- IEEE 802.5：令牌环访问控制方法与物理层规范。
- IEEE 802.6：城域网（MAN）访问控制方法与物理层规范。
- IEEE 802.7：宽带局域网访问控制方法与物理层规范。
- IEEE 802.8：FDDI 访问控制方法与物理层规范。
- IEEE 802.9：综合语音和数据的访问方法和物理层规范。
- IEEE 802.10：网络安全与加密访问方法和物理层规范。
- IEEE 802.11：无线局域网访问控制方法与物理层规范。
- IEEE 802.12：100VG-AnyLAN 快速局域网访问控制方法与物理层规范。
- IEEE 802.14：利用有线电视（Cable-TV）的宽带通信标准。
- IEEE 802.15：无线个人区域网（WPAN）规范。
- IEEE 802.16：宽带无线网标准。

这些标准间的关系如图 1-50 所示，其中 802.4、802.5、802.12 已经淘汰。



图 1-50　IEEE 802 标准关系图

1.5.3.2　IEEE 802.3 协议

1．帧结构

早期 MAC 帧规定的载荷是 LLC 帧，但这种格式现在已不再使用。现在普遍使用的帧格式是直接封装 IP 包的格式，如图 1-51 所示。

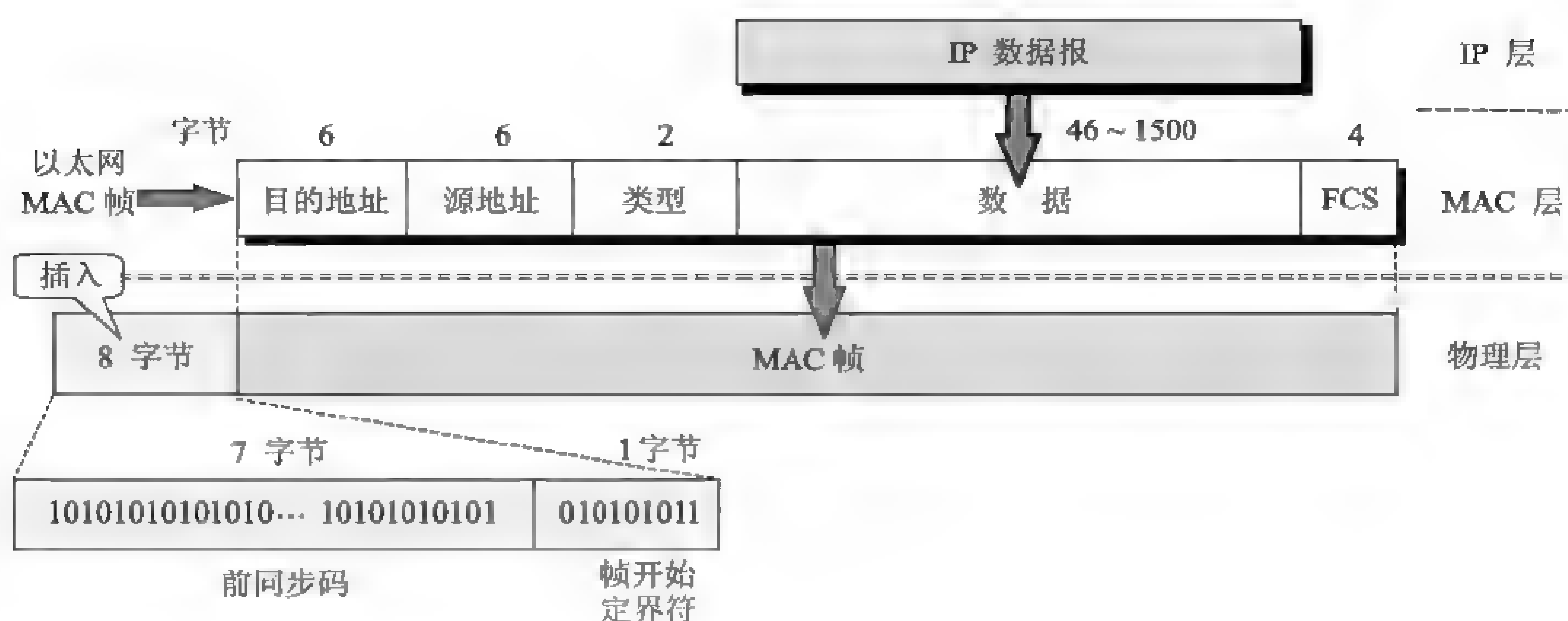


图 1-51 802.3 帧格式

2．FCS 生成方式

帧校验和（FCS）按 CRC-32 生成 4 字节的 CRC 校验和。其生成多项式为：

$$G(x)=x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^{8}+x^{7}+x^{5}+x^{4}+x^{2}+x+1$$

3．适应性策略

采用 CSMA/CD 访问控制方式，使用截断的二进制指数退避算法确定随机延迟时间，重试或发送时选择在时间片开始时刻进行，不跨越时间片，以减少冲突机会。

4．数据编码

原始的 802.3 物理层采用曼彻斯特编码，但 802.3u 采用 4B/5B 编码，802.3z 采用 8B/10B 编码，802.3ae 采用 64B/66B 编码。

1.5.4 高速局域网

1.5.4.1 快速以太网（100Mbps）

快速以太网（fast ethernet）特指数据率为 100Mbps 的以太网，数据率不低于 100Mbps 的以太网统称高速以太网。1995 年， IEEE 802 委员会正式批准快速的协议标准为 IEEE 802.3u（100Base）。

快速以太网保持传统的 Ethernet 帧结构与介质访问控制方法不变，在 LLC 子层使用 IEEE 802.2 标准，MAC 子层使用 CSMA/CD 方法。只在物理层做了必要的调整，重新定义了新的物理层标准，并提供 10Mbps 与 100Mbps 速率自动协商功能。

1．MII 结构

100Base-T 标准定义了介质无关接口（Media Independent Interface，MII），它将 MAC 子层与物理层分隔开来。图 1-52 给出了介质专用接口 MII 结构。这样，物理层在实现

100Mbps 速率时，传输介质和信号编码方式的变化不会影响 MAC 子层。MII 向上通过与 MAC 子层的接口提供载波侦听信号与冲突检测信号，向下支持 10Mbps 与 100Mbps 速率的接口，以及与集线器交换控制信息的功能。

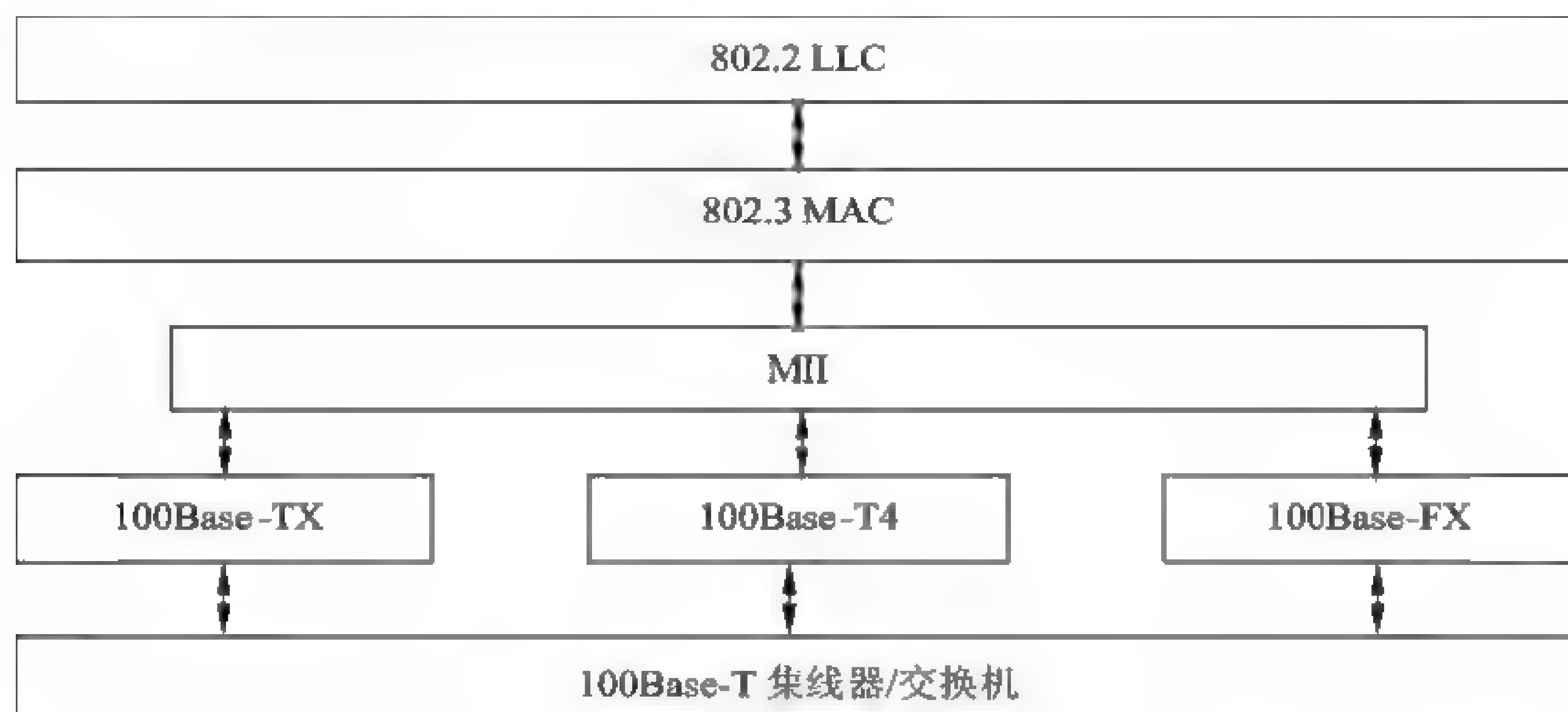


图 1-52　介质无关接口 MII 结构

2．Fast Ethernet 的介质接口

l00Base-T 标准可以支持多种传输介质。目前，100Base-T 有以下三种传输介质标准：100Base-TX、100Base-T4 与 100Base-FX。

1）100Base-TX

100Base-TX 使用 2 对 5 类非屏蔽双绞线(UTP)，最大长度为 100m，一对双绞线用于发送，另一对双绞线用于接收，数据传输采用 4B/5B 编码方法，采用全双工方式工作。

2）100Base-T4

100Base-T4 使用 4 对 3 类非屏蔽双绞线，最大长度为 100m，三对双绞线用于数据传输，一对双绞线用于冲突检测，数据传输采用 8B/6T 编码方法，采用半双工方式工作。

l00Base-T4 是针对目前很多建筑物以及按结构化布线方法，使用质量较差的 3 类非屏蔽双绞线而设计。数据分在三对双绞线中传输，每条双绞线的有效速率为 33.3Mbps。这种方式现在较少使用。

3）100Base-FX

100Base-FX 使用两条光纤，最大长度为 415m，一条光纤用于发送，另一条光纤用于接收，数据传输采用 4B/5B-NRZI 编码方法，采用全双工方式工作。

3．4B/5B 编码方法

l0Base-T 数据传输采用曼彻斯特编码方法，传输速率为 l0Mbps，时钟频率是 20MHz。其编码效率只有 50%。如果 l00Base-TX 仍采用曼彻斯特编码方法，则时钟频率就需要达到 200MHz。从电路实现的角度来看，系统造价将会大幅度上升。4B/5B 编码方法是将

4b 数据变换成 5b 的码字。本来 5b 可以表示 32 种状态，但只选取其中 16 种状态表示 4 位数据，这样编码效率达到 80%。

4．全双工与半双工工作模式

快速以太网支持全双工与半双工两种工作模式，这是它与传统以太网一个很大的区别。传统以太网的节点通过一个连接点接入同轴电缆，或通过一对双绞线接到集线器或交换机。在这种结构中，节点可以利用这条通道发送和接收数据，但是它在发送数据时不能同时接收，在接收数据时也不能同时发送，因此只能是以半双工方式工作。

如果要实现全双工工作，主机需要通过网卡的两个通道，例如两对双绞线或两根光纤，其中一对双绞线用于发送数据，而另一对双绞线用于接收数据，或是一根光纤用于发送数据，而另一根光纤用于接收数据。这与传统以太网的连接方式不同，它是一种点-点连接方式。支持全双工模式的快速以太网一定是星型结构。

点-点连接方式不存在争用问题，因此不需要采用 CSMA/CD 介质访问控制方法。采取全双工、点-点连接方式的快速以太网，由于发送与接收可以同时进行，其数据率是单双工时的两倍。同时，支持全双工方式的交换机可以自由混接不同速率的以太网网卡，并实现不同速率之间的互联互通。

5．10Mbps 与 100Mbps 速率自动协商功能

快速以太网支持 10Mbps 与 100Mbps 速率网卡的速率自动协商，能更好地与 10Base-T 的以太网兼容。

自动协商具有以下功能：

（1）自动确定非屏蔽双绞线的远端设备使用的是半双工（CSMA/CD）的 10Mbps 工作模式，还是全双工的 100Mbps 工作模式。

（2）向其他节点发布远端设备的工作模式。

（3）与远端连接设备交换工作模式相关参数，协调和确定双方的工作模式。

（4）自动选择共有的最高性能的工作模式。

自动协商功能只能用于使用双绞线的以太网，自动协商过程需要在 500ms 内完成。

各种模式，性能越高，优先级越高，优先采用高优先级的性能模式。这些协议按性能从高到低的顺序如下：

（1）100Base-TX 或 100Base-FX 全双工模式

（2）100Base-T4

（3）100Base-TX 半双工模式

（4）10Base-T 全双工模式

（5）10Base-T 半双工模式

自动协商功能是通过链路两端设备交换 100Base-T 定义的“基本链路代码字”来实现的。基本链路代码字长度为 16b，其格式为：

S0	S1	S2	S3	S4	A0	A1	A2	A3	A4	A5	R	R	RF	ACK	NP

其中：S0～S4 00001 表示使用的是 IEEE 802.3 协议，A0 表示 10Base-T 半双工，A1 表示 10Base-T 全双工，A2 表示 100Base-T 半双工，A3 表示 100Base-TX 全双工，A4 表示 100Base-T4 半双工，A5 表示支持帧流控，RF 表示远端故障，ACK 表示确认。

1.5.4.2 千兆以太网

随着数据量的增加，用户对以太网速度要求越来越高，快速以太网已经不能满足要求。于是在 1998 年发布了千兆以太网标准 IEEE 802.3z。其规划了用以太网组建企业网的全面解决方案：桌面系统采用传输速率为 10～100Mbps 的以太网，部门级网络系统采用传输速率为 100Mbps 的快速以太网，企业主网络系统采用传输速率为 1Gbps 的千兆以太网。由于传统以太网与快速以太网、千兆以太网有很多相同点，并且很多企业已大量使用 10Mbps 的以太网，因此当局域网系统从传统以太网升级到 100Mbps 或 1Gbps 时，网络技术人员不需要重新培训，只需对硬件进行升级即可，应用系统无须进行任何变更。因此，千兆以太网有着非常广泛的应用前景。随着千兆以太网技术的成熟，现已成为大、中型局域网系统主干网的首选方案。

1．千兆以太网的特点

（1）保持与现有以太网标准的向下兼容。IEEE 802.3z 标准在 LLC 子层使用 IEEE 802.2 标准，在 MAC 子层使用 CSMA/CD 方法，保持同样的帧结构与帧的最大长度，支持单播与组播两种传输模式，只在物理层进行修改。

（2）所有的配置都采用点-点连接方式。

（3）能与 10Mbps、100Mbps 以太网自动实现速率匹配，互联互通。

2．千兆以太网的物理层协议

IEEE 802. 3z 标准包括 4 种物理层标准：1000Base-LX、1000Base-SX、1000Base-CX 与 1000Base-T。其中，1000Base-LX、1000Base-SX、1000Base-CX 统称为 1000Base-X。

1）1000Base-LX

1000Base-LX 使用光纤作为传输介质构成星型拓扑。在采用多模光纤时，半双工工作模式光纤最大长度为 316m，全双工工作模式光纤最大长度为 550m。在使用单模光纤时，半双工模式的光纤最大长度为 316m，全双工模式的光纤最大长度为 5000m。数据传输采用 8B/10B 编码方法。

2）1000Base-SX

1000Base-SX 使用光纤作为传输介质构成星型拓扑。在采用 62.5μm 多模光纤时，半双工和全双工模式的光纤最大长度均为 275m。在使用 50μm 多模光纤时，半双工和全双工模式的光纤最大长度均为 550m。数据传输采用了 8B/10B 编码方法。

3）1000Base-CX

1000Base-CX 使用特殊的屏蔽双绞线构成星型拓扑。半双工模式的双绞线最大

长度为 25m，全双工模式的双绞线最大长度为 50m。数据传输采用了 8B/10B 编码方法。

4）1000Base-T

1000Base-T 使用 4 对 5 类非屏蔽双绞线构成星型拓扑。双绞线最大长度为 100m，使用 RJ-45 接口。数据传输采用 PAM5 编码方法。

3．千兆以太网对 IEEE 802.3 协议的调整

1）冲突窗口时间与最小帧长度的调整

传统以太网的 CSMA/CD 机制要求发送节点在一个冲突窗口，即发送 512b 时间（51.2μs）内检测出是否发生冲突，因此冲突窗口的时间长短直接影响到一个网段的量大长度。传统以太网与快速以太网将冲突窗口规定为 51. 2μs，千兆以太网的发送速率提高了 100 倍，发送同样长度帧的时间就仅是原来的 1/100。由于信号在传输介质中传播的速度不变，为了保证能在一帧的发送过程中检测到冲突，则网段的最大长度仅是 1/100，即千兆以太网网段的最大长度就要缩小到 10m 甚至 1m 以下。因此必须对 CSMA/CD 机制进行修改，IEEE 802. 3z 标准将发送 512b 的时间修改为发送 512B 的时间，即将原来的最小帧长度为 64B 修改为 512B，但最大长度仍为 1518B，这样可以保持千兆以太网网段的最大长度与之前的以太网一致。

2）帧突发处理

由于将帧的最短长度确定为 512B，当要发送较短的帧时，必然发送大量填充的无用信息（称为载波扩展），导致信道利用率降低。为此，千兆以太网允许各个节点有选择地利用突发模式（burst mode）来发送帧。

突发模式基本思想是：将多个小于 512B 的短帧组合在一起，拼接成一个大于 512B 的正常帧发送，在该正常帧内的各个短帧之间，设置一个帧间隔标志 IFG 进行分隔。

突发模式处理过程是：当一个节点试图发送一个突发帧时，首先设置一个“突发定时器”，并在开始发送突发帧时启动定时器。第一个短帧（小于 512B）发送完毕准备发送载波扩展时，如果没有检测到冲突，且此时还有新的短帧需要发送，则启动突发模式发送。这时，如果突发定时器时间未到，则在一个 IFG 后继续发送后续帧。如果节点在发送第一个帧的过程中出现了冲突，需要执行正常的后退延迟操作并停止发送。如果发送的第一个帧和载波扩展没有出现冲突，这时就可以连续地发送后续帧。最大突发帧最长能够占用 8192B 的发送时间。这个值是节点从开始发送第一帧到开始发送最后一帧之间的最大时间。因此，帧突发的最大持续时间等于突发帧长度的发送时间加上 1 个最大帧长度的发送时间，即 8192+1518+8＝9718 (B) 的发送时间。显然，在采用帧突发处理之后，半双工模式千兆以太网的信道利用率大大提高。在 1000Mbps 传输速率的情况下，半双工状态与 CSMA/CD 的机制不可取，因此应采用点-点连接的全双工模式。

IFG 起到分隔多个帧的作用，同时也使接收节点利用此段时间使设备能恢复以接收下一帧。

4．千兆介质专用接口 GMII

IEEE 802. 3z 标准定义了千兆介质专用接口 GMII，如图 1-53 所示，它将 MAC 子层与物理层分隔开来，以保证在实现 1000Mbps 的传输速率时，物理层使用的传输介质和信号编码方式的变化不会影响 MAC 子层。

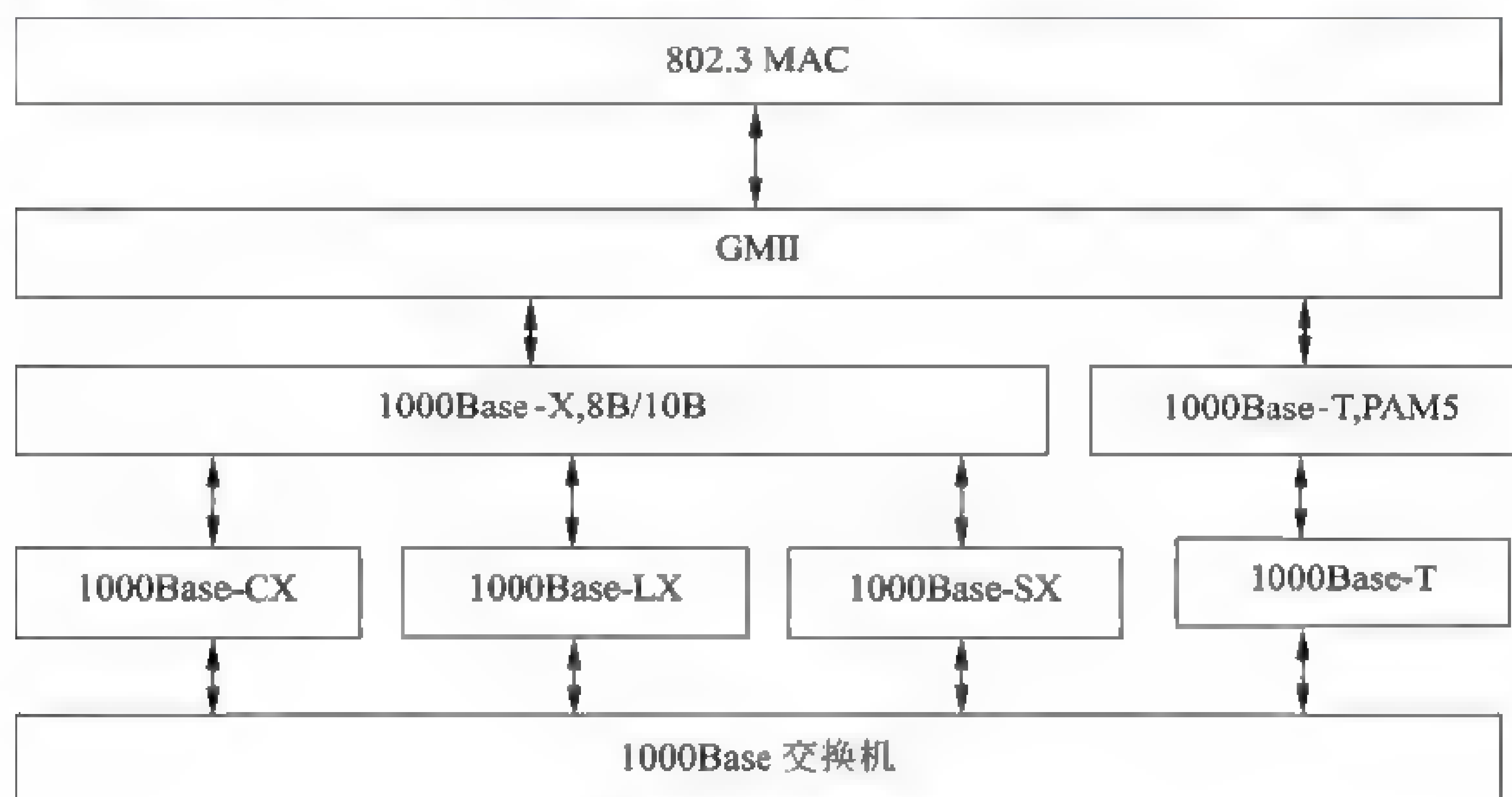


图 1-53　GMII 结构

5．自动协商机制

千兆以太网延续了自动协商的概念，并将它扩展到光纤连接中。千兆以太网自动协商有两种形式：一种用于 1000Base-X，另一种用于 1000Base-T。

1000Base-X 的自动协商用于协调链路两端节点是半双工还是全双工操作，以及流量控制是对称还是非对称的。1000Base-X 的协商严格限定在 1000Mbps 速率，不能在不同的速率之间进行协商。链路两端设备必须安装相同类型的发送器和接收器，不同的发送器和接收器之间不兼容。1000Base-X 使用 8B/10B 编码作为链路代码字实现自动协商。1000Base-X 使用与快速以太网相同的协议与报文格式。

1000Base-T 使用叫做快速链路脉冲的 FLP 交换各自传输能力的通告。FLP 可以让对端知道源端的传输能力是怎样的。当交换 FLP 时，两个站点根据以下从高到低的优先级侦测双方共有的最佳方式。

- 1000Base-T 全双工
- 1000Base-T 半双工
- 100Base-T2 全双工
- 100Base-TX 全双工

- 100Base-T2 半双工
- 100Base-T4 半双工
- 100Base-TX 半双工
- 10Base-T 全双工
- 10Base-T 半双工

1.5.4.3 万兆以太网

随着宽带城域网的建设需要和用户对带宽越来越高的需求，以及基于光纤的密集波分复用技术的成熟，对 1Gbps 的千兆以太网进行升级，但仍能保持以太网特性，速率再提高 10 倍且能用于主干网的技术，称为非常自然的选择，这种选择导致 10Gbps 以太网（万兆以太网）的诞生。

IEEE 在 1999 年 3 月成立了高速研究组（High Speed Study Group，HSSG），其任务是致力于 10Gbps 以太网的研究。2002 年 6 月，IEEE 802 委员会通过 10Gbps 以太网的正式标准。在 10Gbps 以太网标准的制定过程中，遵循了技术可行性、经济可行性与标准兼容性的原则，目标是将以太网从局域网范围扩展到城域网与广域网范围，成为城域网与广域网的主干网的主流技术之一。因此，万兆以太网不再简单地称为局域网，它既是局域网，也是广域网。

1．10Gbps 以太网的主要特点

10Gbps 以太网的主要特点如下：

（1）帧格式与 10Mbps、100Mbps 和 1Gbps 以太网的帧格式相同。

（2）保留 IEEE 802.3 标准对以太网最小帧长度和最大帧长度的规定，使用户在将其已有的以太网升级时，仍然便于和较低速率的以太网进行通信。

（3）传输介质不再使用铜质的双绞线，而只使用光纤，以便能在城域网和广域网范围内工作。

（4）只工作在全双工方式，因此不存在介质争用的问题。由于不需要使用 CSMA/CD 工作机制，这样传输距离不再受冲突检测的限制。

2．10Gbps 以太网的物理层协议

10Gbps 以太网的物理层使用光纤通道技术，因此它的物理层协议需要进行修改。10Gbps 以太网有两种不同的物理层标准：10Gbps 以太网局域网标准（Ethernet LAN，ELAN）与 10Gbps Ethernet 广域网标准（Ethernet WAN，EWAN），其物理层标准包括如下几项。

1）10000Base-ER

10000Base-ER 是 IEEE 802.3ae 标准中，在一对光纤中传输 10Gbps 以太网局域网信号的物理层标准。10000Base-ER 的网络拓扑是星型结构，局域网物理层（LAN PHY）采用 1550nm 波长激光。在使用 10μm 单模光纤时，光纤最大长度为 40km。数据传输采

用 64B/66B 编码方法。

2）10000Base-EW

10000Base-EW 是 IEEE 802.3ae 标准中，在一对光纤中传输 10Gbps 以太网局域网信号的物理层标准。10000Base-EW 的网络拓扑是星型结构，物理层采用 1550nm 波长激光。在使用 10μm 单模光纤时，光纤最大长度为 40km。数据传输采用 64B/66B 编码方法。

3）10000Base-LR

10000Base-LR 是 IEEE 802.3ae 标准中，在一对光纤中传输 10Gbps 以太网广域网信号的物理层标准。10000Base-LR 的网络拓扑是星型结构，物理层（LAN PHY）采用 1310nm 波长激光。在使用 10μm 单模光纤时，光纤最大长度为 40km。数据传输采用 64B/66B 编码方法。

4）10000Base-L4

10000Base-L4 是 IEEE 802.3ae 标准中，在一对光纤中传输 10Gbps 以太网广域网信号的物理层标准。10000Base-L4 的网络拓扑是星型结构，物理层采用 1310nm 波长激光。在使用 62. 5μm 或 50μm 多模光纤时，光纤最大长度分别为 240m 与 300m。在使用 10μm 单模光纤时，光纤最大长度为 40km。数据传输采用 8B/10B 编码方法。

5）10000Base-SR

10000Base-SR 是 IEEE 802.3ae 标准中，在一对光纤中传输 10Gbps 以太网局域网信号的物理层标准。10000Base-SR 的网络拓扑是星型结构，物理层采用 850nm 波长激光。在使用 62.5μm 或 50μm 多模光纤时，光纤最大长度分别为 35m 与 300m。数据传输用 64B/66B 编码方法。

6）10000Base-SW

10000Base-SW 是 IEEE 802.3ae 标准中，在一对光纤中传输 10Gbps 以太网广域网信号的物理层标准。10000Base-SW 的网络拓扑是星型结构，物理层采用 850nm 波长激光。在使用 62.5μm 或 50μm 多模光纤时，光纤最大长度分别为 35m 与 300m。数据传输采用 64B/66B 编码方法。

由于 10Gbps 以太网需要兼顾 LAN 与 WAN 两种应用环境，而二者在信号传输的诸多方面明显不同，因此 IEEE 802.3ae 标准为 LAN 与 WAN 分别制定相应的物理层标准。两种物理层标准的共性是：共用 MAC 层，采用光纤作为传输介质，仅支持全双工模式，不使用 CSMA/CD 机制。

（1）10Gbps 以太网局域网物理层协议的特点。

由于 10Gbps 以太网需要与 1Gbps 的千兆以太网兼容，因此 10Gbps 以太网局域网的物理层与 MAC 层，必须允许工作在 10Gbps 或 1Gbps 两种速率。10Gbps 以太网交换机必须具备将 10 路 1Gbps 的千兆以太网信号复用的能力，即支持 10 路 1Gbps 的千兆以太网端口。这样，可以平滑地将 1Gbps 的千兆以太网、100Mbps 的百兆以太网与 10Mbps 的以太网，以最小代价升级到一个大型、宽带局域网中，将网络的覆盖范围扩大到 40km。

（2）10Gbps 以太网广域网物理层协议的特点。

10Gbps 以太网的广域网物理层应该符合光纤通道技术速率体系 SONET/SDH 的 OC-192/STM-64 标准。OC-192 的传输速率为 9.58464Gbps，而不是精确的 10Gbps。在这种情况下，10Gbps 以太网帧将插入 OC-192/STM-64 帧的有效载荷中，以便与光纤传输系统相连接。因此，10Gbps 以太网广域网的 MAC 层需要通过 10Gbps 介质独立子层 XGMII 接口实现 9. 58464Gbps 的速率匹配。

3．10Gbps 以太网对 IEEE 802.3 协议的调整

由于要考虑在城域网和广域网中的应用，10Gbps 以太网必须充分考虑以太网帧信号远距离传输的要求，因此 10Gbps 以太网在物理层实现方法、帧格式、MAC 工作速率及适配策略等方面与传统以太网必定存在差别，需对传统以太网进行一些调整。

1）MAC 帧格式的调整

由于 10Gbps 以太网将多个帧封装在一个 OC-192 帧中进行传输，因此必须解决如何标识多个以太网帧的问题。在 10Gbps 以太网中，它是通过修改 MAC 帧格式来实现的。图 1-54 是新的 10Gbps 以太网帧格式。

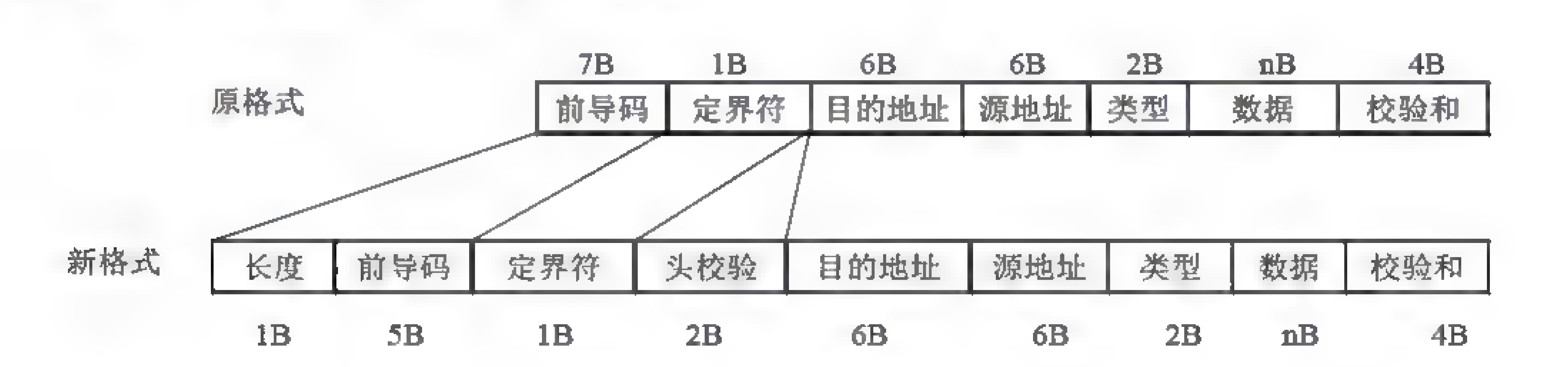


图 1-54　10Gbps 以太网帧格式

10Gbps 以太网帧格式是在原有 MAC 帧格式上增加了 2B 的“长度”字段，代替了传统 MAC 帧的前导码的前两个字节。由于最大帧长度为 1518B，因此需要 2B 的长度字段可以（最多 2^{11}B 即 2048B）。同时，在原帧前定界符与目的地址之间增加了一个 2B 的“帧头校验”字段，对它前面的长度、前导码与帧前定界符的 8 个字节进行 CRC-16 校验。

10Gbps 以太网对帧的修改只是针对封装到 OC-192 帧时，它只对物理层的传输过程有效。当发送端的 MAC 层将帧传送到物理层封装到 OC-192 帧时，需要增加帧之间的标识，这时才需要修改原 MAC 帧的结构。在物理传输介质中传输的是 OC-192 帧。当接收端的物理层接收到一个 OC-192 帧后，需要通过拆分 OC-192 帧还原出原 MAC 帧，然后将还原的 MAC 帧提交给 MAC 层处理。这个封装与拆分 OC-192 帧的过程，对源节点和目的节点的 MAC 层是透明的。这种修改工作是在物理层进行的，并没有真正修改 MAC 帧结构。事实上，10Gbps 以太网与之前的以太网的帧结构是相同的。

2）局域网和广域网的速率匹配

10Gbps 以太网局域网与广域网物理层的数据传输速率不同，局域网的数据传输速率是 10Gbps，而广域网的数据传输速率是 9.58464Gbps。但是，这两种速率的物理层共用 MAC 层。MAC 层的工作速率是按 10Gbps 设计的。因此，10Gbps 以太网必须采取一种调整策略，通过 10G 介质专用接口(10GMII 或 XGMII)，将 MAC 层的工作速率由 10Gbps 减低到 9.58464Gbps，使它能与物理层的数据传输速率匹配。现在使用的调整策略大致有以下三种：

① 通过 10GMII 接口发送 HOLD 信号，让 MAC 层在一个时钟周期中停止发送。

② 在每个帧间隙时间 IPG 中，由物理层向 MAC 层发送 Busy Idle 信号。这时 MAC 层暂停发送数据。当物理层向 MAC 层发送 Normal Idle 信号后，MAC 层重新开始发送数据。

③ 采用帧间隙时间 IPG 延长机制。MAC 层每次传输完一个帧后，根据平均数据速率动态调整 IPG 间隔。

10Gbps 以太网能很好地实现与 SONET/SDH 传输网络的互联，可以完成从局域网到城域网、广域网的无缝连接和扩展。

1.5.5　无线局域网

1.5.5.1　Wi-Fi (802.11)无线局域网

1．无线局域网概述

无线局域网（Wireless LAN，WLAN）是一种以无线通信为传输方式的局域网，是实现移动计算机网络的关键技术之一。无线局域网以微波、激光与红外线等无线电波作为传输介质，来部分或全部代替传统局域网中的有线传输介质，实现了移动计算机网络中移动节点的物理层与数据链路层功能，并为移动计算机网络提供物理接口。无线局域网的发展速度相当快。目前，300Mbps 传输速率的系统已经成熟，而速率更高的系统正在研究中。

无线局域网不仅能满足移动和特殊应用领域的需求，还能覆盖有线网络难以覆盖的地方，如受保护的建筑物、不能或不方便铺设有线介质的地方、临时性场所等。

无线局域网的应用领域主要有以下 4 个方面：作为传统有线局域网的扩充、建筑物之间的互联、漫游访问与特殊网络。

2．WLAN 传输介质

无线局域网使用的是无线传输介质，按所采用的传输技术可以分为三类：红外线局域网、扩频局域网和 OFDM（正交频分多路复用）局域网。

红外线局域网的数据传输有三种基本技术：定向光束红外传输、全方位红外传输与漫反射红外传输。红外线波长在 850～950nm 之间，数据传输速率为 1Mbps 或 2Mbps。

红外线传输的优点是不能进行重复攻击，缺点是，传输距离小，且不能绕过障碍物。

扩频无线局域网的数据传输有两种基本技术：跳频扩频 FHSS 与直接序列扩频 DSSS。

跳频扩频 FHSS 使用的是免申请的扩频无线电频率，包括 902～928MHz（915MHz 频带、2.4～2.485GHz（2.4GHz 频带）、5.725～5. 825GHz（5.8GHz 频带）三个频带。直接序列扩频 DSSS 使用 2.4GHz 的工业、科学与医药专用的 ISM 频段。目前扩频无线局域网的数据传输速率都在 11Mbps 以下。

OFDM 无线局域网是将无线信号分成多路正交的信号，合在一起传输。由于采用多路复用技术，提高了数据率，可以达到 54Mbps 以上，采用域扩展技术可以达到 108Mbps，配合使用多天线（MIMO），可以达到 300Mbps 以上。

3．WLAN 的网络结构

无线局域网的一般结构如图 1-55 所示，由一个访问点 AP 和若干移动主机组成一个基本服务集 BSS，多个 BSS 组成一个扩展服务集 ESS。其中 AP 一般通过有线方式与后端网络或 Internet 互联。

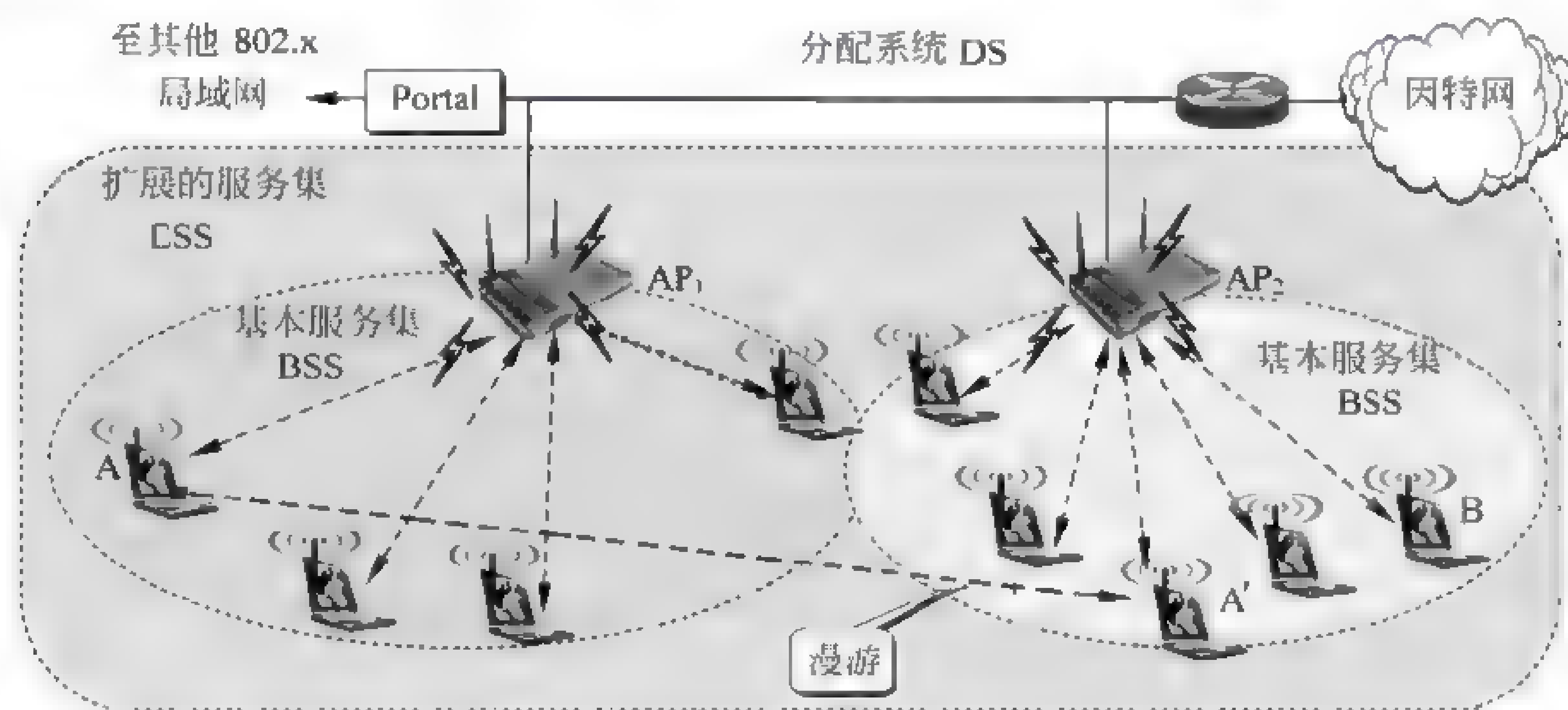


图 1-55　无线局域网的一般结构

无线主机可以从一个 BSS 漫游到另外一个 BSS，整个 BSS 甚至整个 ESS 都可以移动，例如在轮船、火车、飞机上的无线局域网，如图 1-56 所示。

4．WLAN 访问控制方式

无线局域网的访问控制方式用于控制各移动主机与 AP 之间或主机与主机之间的通信。主要有两种方式：点协调功能（Point Coordination Function，PCF）和分布式协调功能（Distributed Coordination Function，DCF）。

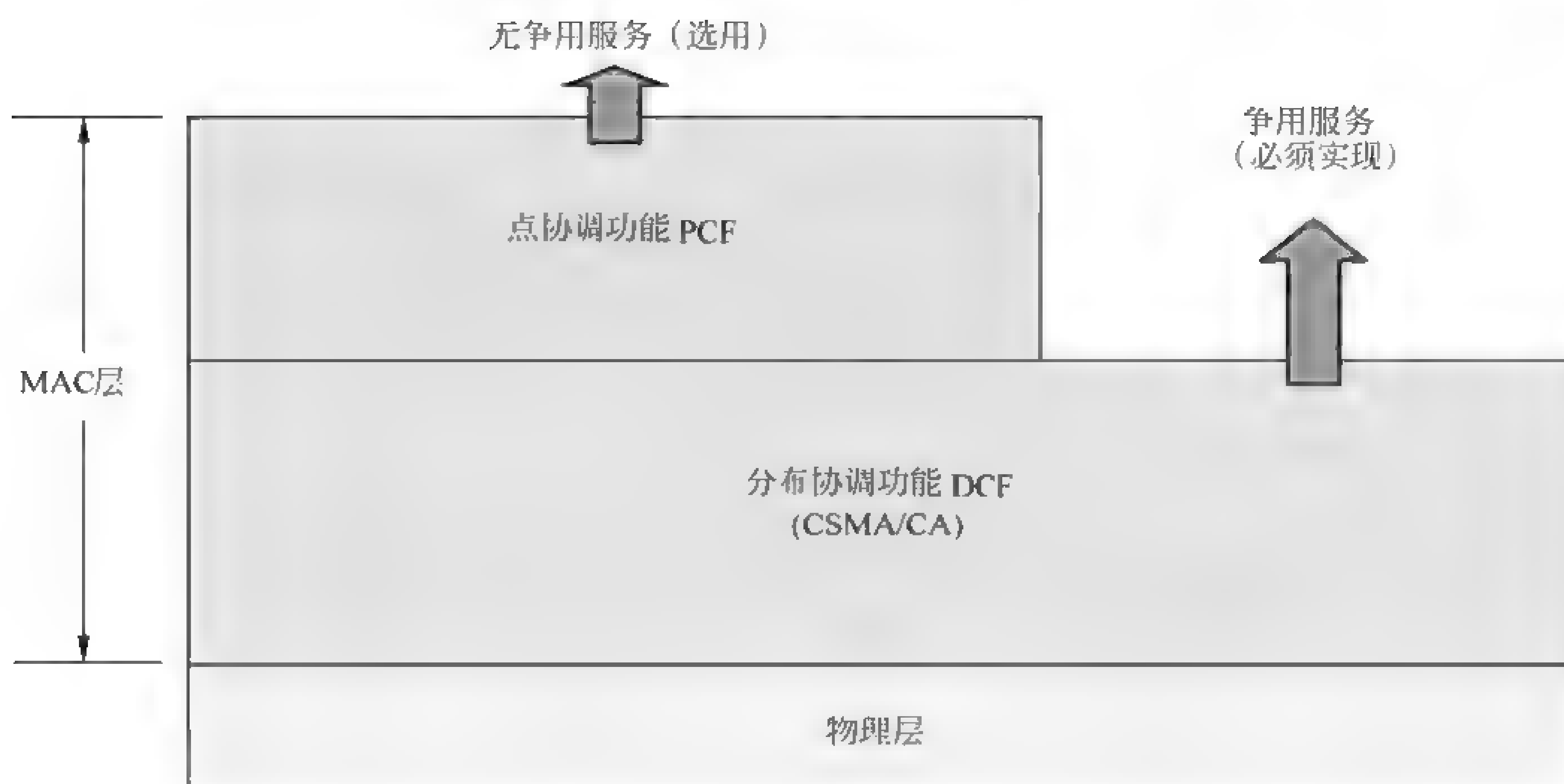


图 1-56　WLAN 访问控制方式

点协调功能（PCF）的原理是：AP 发送数据时可以直接发送，移动主机要发送数据必须等待 AP 的通知。AP 轮询各移动主机有无数据发送，若无，则轮询下一个移动主机，若有，则通知其发送。此时，其他主机不能发送，但可以接收。

分布式协调功能 DCF 的原理如下：

① 发送站点先监听。若没有信号在传送（空闲），再等待一个帧间隔时间（Interframe Spaces，IFS），若仍然空闲，则立即发送。

② 若有信号在传送（忙），则继续监听，直到介质上的传输结束。

③ 一旦当前介质上的传输结束，再延时一个 IFS 时间。若空闲，立即发送，否则调用截断的二进制指数后退算法随机延迟一段时间后转①。

该方式被称为 CSMA/CA 控制方式。

5. WLAN 协议

目前 WLAN 广泛使用的协议是 IEEE 802.11 协议。

1）IEEE 802.11 协议簇

已经发布的 IEEE 802.11 系列的标准主要有以下一些。

- IEEE 802.11：2.4GHz 红外线或扩频物理层、MAC 子层协议，1Mbps 或 2Mbps。
- IEEE 802.11a：5GHz OFDM 物理层、MAC 子层协议，54Mbps。
- IEEE 802.11b：2.4GHz 扩频（DSSS）物理层、MAC 子层协议，11Mbps。
- IEEE 802.11g：2.4GHz OFDM 物理层、MAC 子层协议，54Mbps。
- IEEE 802.11n：2.4GHz OFDM MIMO 物理层、MAC 子层协议，300Mbps。
- IEEE 802.11i：WLAN 安全机制。

2）IEEE 802.11 帧结构

802.11 协议规定的数据帧的格式如图 1-57 所示。

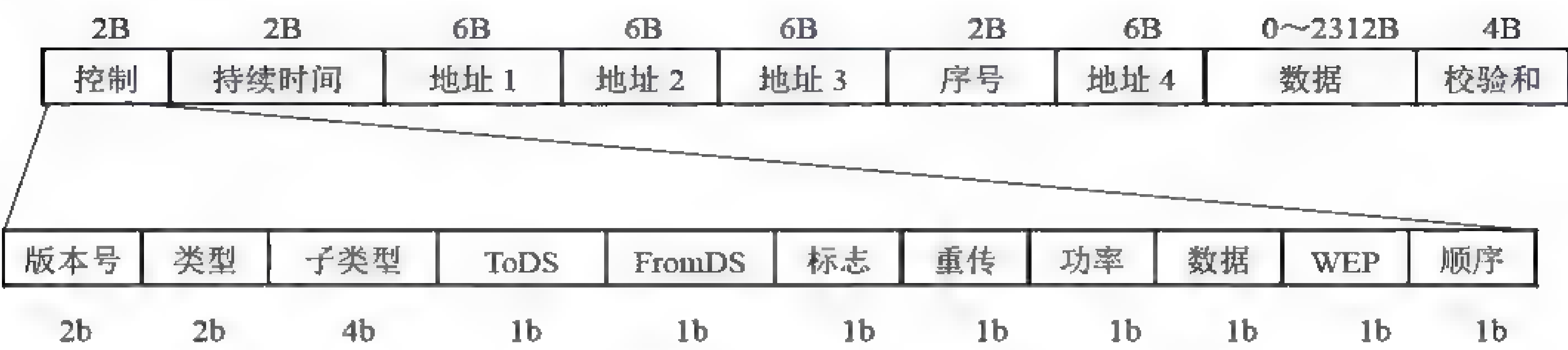


图 1-57　802.11 帧格式

控制：由多个子域组成，完成帧控制功能。

持续时间：表示占用信道的持续时间。

地址：共有 4 个地址，表示基本服务集 BSS 的地址、源地址、目的地址、发送站地址与接收站地址等，具体含义由 ToDS、FromDS 标志位确定。

序号：表示节点发送的协议数据单元的顺序号。

数据域：对应高层数据，长度（0～2312B）可变。

校验和：帧校验和。

3）802.11 工作原理概述

802.11 的 MAC 层采用 CSMA/CA 控制发送与接收。每一个发送节点在发送帧之前需要先侦听信道。如果信道空闲，节点可以发送帧。发送节点在发送完一帧之后，必须再等待一个短的时间间隔，检查接收站是否发回帧的确认 ACK。如果接收到确认，则说明此次发送没有出现冲突，发送成功。如果在规定的时间内没有接收到确认，表明出现冲突，发送失败，重发该帧。直到在规定的最大重发次数之内，发送成功。这个时间间隔叫做帧间隔（IFS）。帧间隔 IFS 的长短取决于帧类型。高优先级帧的帧间隔 IFS 短，因此可以优先获得发送权。常用的帧间隔 IFS 有三种：

- 短帧间隔（Short IFS，SIFS）
- 点帧间隔（PIFS）
- 分布帧间隔（Distributed IFS，DIFS）

点帧间隔 PIFS 与分布帧间隔 DIFS 也叫做点协调功能帧间隔与分布协调功能帧间隔。

短帧间隔 SIFS 用于分隔属于一次对话的各帧，如确认 ACK 帧。它的值与物理层相关。例如 IR 的 SIFS 为 7μs；DSSS 的 SIFS 为 10μs；FHSS 的 SIFS 为 28μs。点协调功能帧间隔 PIFS 的长度等于 SIFS 值加上一个 50μs 的时间片值，FHSS 的 PIFS 值为 78μs。分布协调功能帧间隔 DIFS 最长，它等于在 PIFS 值上再加一个 50μs 的时间片值，即 FHSS

的 DIFS 值为 128μs。

4）IEEE 802.11 站点切换

用户终端（STA）会定期地收集无线信号，搜索可用的 AP 接入点信息。当发现有性能更好的 AP 时（从一个 BSS 移动到另一个 BSS 或有新的 AP 加入），用户终端将启动切换过程，进入切换流程，连接到该 AP。具体的流程如下。

第一步，STA 通过 Re-Association Request 发起切换过程。

第二步，新 AP 发送 IAPP_Move_Notify（IAPPmsg）消息到旧 AP。

第三步，旧 AP 发送 IAPP_Move_Reply（IAPPmsg）消息到新 AP，其中包含 STA 用户信息。

第四步，新 AP 到 AS 中登记为该 STA 的新接入点。

第五步，AS 回复相关的信息给新 AP。

第六步，当 STA 下网时，向 AS 发送 IAPP_usr_offline 消息，通知用户下网。

第七步，AS 向新 AP 发送该 STA 下网的消息，并附带相关的用户信息。

1.5.5.2　蓝牙技术

1994 年，瑞典 Ericsson 公司与 IBM、Intel、Nokia 和 Toshiba 等 4 家公司共同发起，开发一个用于将计算机与通信设备、附加部件和外部设备，通过短距离、低功耗、低成本的无线信道连接的无线标准。这个项目被命名为蓝牙（bluetooth）。

蓝牙系统的网络结构如图 1-58 所示。

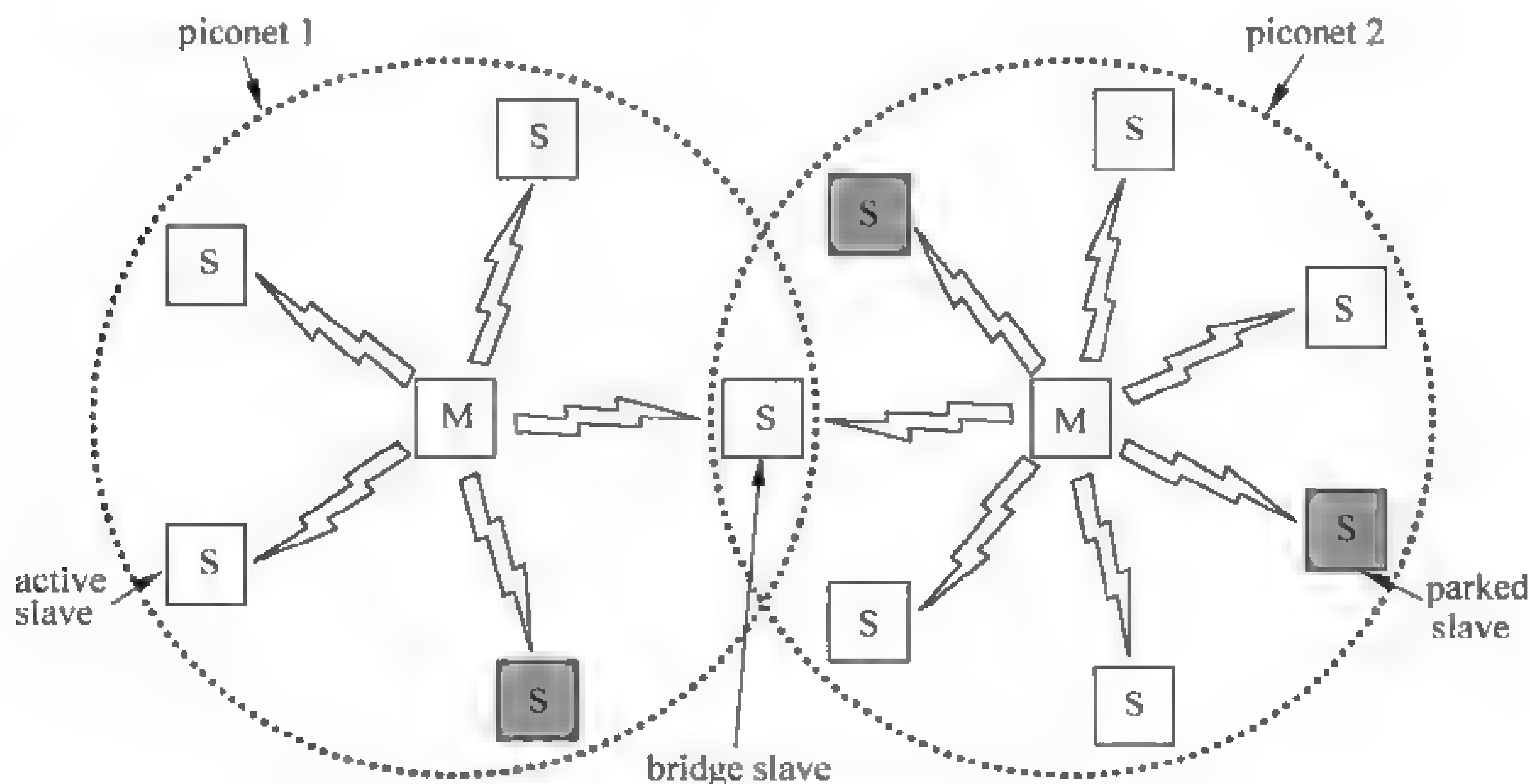


图 1-58　蓝牙的网络结构

蓝牙系统的基本单元是微微网（piconet）。每个微微网都包含一个主节点（master），最多 7 个活动的从节点（active slave），以及可以多达 255 个静观节点（parked slave）。

静观节点是指这样的一类设备，主节点已将它切换到一种低功耗状态，以降低它们的电源消耗。静观设备除了响应主节点的激活或指示信号以外，不做其他任何事情。

在同一房间中可以同时存在多个微微网，它们可以通过一个桥节点连接起来。两个相互连接的微微网成为一个分散网（scatternet）。微微网是一个中心控制的 TDM 系统，主节点控制了时钟，它决定每个时间片分配给哪个设备进行通信。所有通信都在主节点和从节点之间进行，从节点与从节点之间不直接通信。蓝牙系统的设计目标之一是，争取将一个完整的蓝牙芯片的价格降低到 5 美元以下，从而可以大规模地推广使用。

蓝牙 1.0 标准规定主从节点之间的距离不超过 10m，数据率为 720Kbps。2.0 标准有望将数据率提高到 10Mbps，距离延伸到 100m。

1.5.6 虚拟局域网

1.5.6.1 VLAN 的概念

虚拟局域网（VLAN）是由一些 LAN 网段构成的与物理位置无关的逻辑组。VLAN 的形成并没有改变原有网络的拓扑，在用户看来，网络的视图是一致的。

逻辑组之间通过实现互联的网桥或路由器来交换数据。当一个逻辑组的节点要转移到另一个逻辑组时，就需要将节点计算机从一个网段撤出，并将它连接到另一个网段上，这时有可能需要重新进行布线。因此，逻辑组的组成受节点所在网段的物理位置限制。

虚拟局域网是建立在局域网交换机之上的，它以软件方式实现逻辑组的划分与管理，逻辑组中的节点组成不受物理位置的限制。同一逻辑组的成员不一定连接在同一个物理网段上，它们可以连接在同一个局域网交换机上，也可以连接在不同的局域网交换机上，只要这些交换机之间互联就可以。当一个节点从一个逻辑组转移到另一个逻辑组时，只需要简单地通过软件设定来改变逻辑组，而不需要改变它在网络中的物理位置。同一个逻辑组的节点可以分布在不同的物理网段上，但它们之间的通信就像在同一个物理网段上一样。因此，VLAN 是通过软件的方法，逻辑的而不是物理地将节点划分成一个个网段。

目前 VLAN 的主要标准是 IEEE 802.1Q 标准。

1.5.6.2 VLAN 组网方法

1．基于端口划分 VLAN（Port-Based）

指定交换机上的哪些端口组成一个 VLAN。

早期基于端口的 VLAN 成员只能位于同一个交换机中。现在基于端口的 VLAN 支持多个交换机，例如交换机 X 上的端口 1 和端口 2 与交换机 Y 上的端口 3 和端口 4 可以构成一个 VLAN，只要交换机 X 和交换机 Y 连接在一起（堆叠或级联）。

此种方式的优点是直观，缺点是当工作站移动或使用者变更（如更换办公室）时，

需要重新配置交换机。

2．基于 MAC 地址划分 VLAN（MAC-Layer Grouping）

指定一组 MAC 地址构成一个 VLAN，用户属于哪个 VLAN 由其网卡中的 MAC 地址决定。

此种方式的优点是用户/主机可以移动，缺点是更换网卡或主机后，需要重新配置交换机，同时需要管理员记录大量 MAC 地址及其与用户、主机的对应关系。

3．基于网络层地址划分 VLAN（Network-Layer Grouping）

指定一组网络地址（如一组 IP 地址）构成一个 VLAN。

此种方法的优点是用户、主机可以随意移动，缺点是效率较前述方法低，且 IP 地址可冒用，不具有唯一性。

4．基于协议划分 VLAN（Protocol-Based）

指定使用某种协议的节点组成一个 VLAN。

由于目前基本上都使用 TCP/IP 协议，因此这种方式的适用性较低。

5．基于策略划分 VLAN（Policy-Based）

策略源于网络管理，主要是指网络管理行为所遵守的规则。这些规则涉及网络管理员和软硬件系统的禁止、允许、授权等行为，尤其是当网络产生报警信息时，网络和网络管理员应该采取的措施。

策略的内容一般包括以下内容：

（1）作用范围是什么？

（2）规则是什么？

（3）对象是什么？

（4）属性是什么？

（5）对象如何分组？

（6）什么事件触发策略驱动程序？

（7）行为的结果是什么？

可以将使用共同策略的节点组成一个 VLAN。

不论采用哪种方式，一个地址、端口只能划分到一个 VLAN 中。

1.5.6.3　IEEE 802.1Q 与 VTP 协议

1．IEEE 802.1Q 帧格式

IEEE 802.1Q 定义的 VLAN 帧格式如图 1-59 所示，它对以太网帧格式进行了修改，在以太网帧格式中增加 2 个字节，共 4 个部分。

目的地址	源地址	TPID	优先级	CFI	VLAN ID	长度	数据	校验和

图 1-59　802.1Q VLAN 帧格式

目的地址、源地址、长度、数据、校验和为以太网帧的固有字段，TPID、优先级、

CFI、VLAN ID 为 802.1Q 增加的字段，其含义如下。

TPID（tag protocol identifier）：2 字节，是 IEEE 定义的新的类型，表明这是一个加了 802.1Q 标签的帧。TPID 包含了一个固定的值 0x8100。

优先级：3 位，一共有 8 种优先级，0～7，指明数据的优先级。

CFI（canonical format idicator）：1 位，值为 0 说明是规范格式，1 为非规范格式。它被用在令牌环/源路由 FDDI 介质访问方法中来指示封装帧中所带地址的比特次序信息。

VLAN ID：12 位，指明 VLAN 的 ID，一共 4096 个，每个支持 802.1Q 协议的交换机发送出来的数据包都会包含这个域，以指明自己属于哪一个 VLAN。

2．VTP 协议

一个网络使用 VLAN 后需要对穿过多个交换机的 VLAN 进行配置和维护。如果没有一个集中的方法配置和维护 VLAN 信息，网络管理员必须对每一个交换机进行独立的 VLAN 配置。为简化配置和维护工作，思科公司开发了一种 VLANTrunk 协议（VTP）。

VTP 允许在一个单独的设备（VTP 服务器）上配置 VLAN，并把配置信息通过交换网络传递出去。这减少了管理 VLAN 需要的总时间。

在一个 VTP 环境里，一台交换机可以是以下三种不同的角色之一。可以是一台 VTP 服务器，一台 VTP 客户机，或者工作在透明模式。角色决定了交换机在 VLAN 网络中被如何配置。

VTP 有支持多个 VTP 域的能力。每个 VTP 域的客户交换机从该域的 VTP 服务器接收自身的配置信息。在同一个本地网络可以有多个 VTP 域。

1）VTP 服务器

VTP 服务器是每个 VTP 域的根本。服务器是 VTP 域内唯一可以增加、删除、重命名 VLAN 的交换机。当一台未经配置的交换机第一次上电开机的时候，它的默认模式是服务器模式。我们必须把它改成客户机或者透明模式。

VTP 服务器周期性地广播 VTP 域名、VLAN 配置，提供现行的配置修改号。这个修改号是 VTP 域的一部分，它确保 VTP 域内的所有交换机有现行的、正确的 VLAN 配置信息。

当 VLAN 在 VTP 服务器上被创建的时候，和其他 VLAN 配置信息一起存储在服务器的 NVRAM（存储单元）。当交换机重启的时候，配置信息还是被保留。

2）VTP 客户交换机

VTP 客户交换机从 VTP 服务器接收所有客户交换机的配置信息。客户交换机不能删除、添加、重命名 VLAN。当客户交换机加入一个新的 VLAN，VLAN 必须被添加到 VTP 服务器上面去。这样新的 VLAN 才能传递到所有的客户交换机。当新的 VLAN 增加后，客户交换机上的端口会关联到新的 VLAN。

类似 VTP 服务器，客户交换机在 NVRAM 存储 VLAN 配置。然而，不像 VTP 服务

器，当客户交换机重启的时候，所有的 VLAN 配置信息丢失了。交换机启动完成后，需要发送一条 VTP 请求消息给 VTP 服务器，来获取现行的 VLAN 配置。

3）VTP 透明模式

VTP 透明交换机和 VTP 客户交换机不同，VLAN 可以在这些交换机上手工配置。如果配置为 VTP 域的一部分，它们可以从 VTP 服务器接收 VLAN 配置信息。然而，它们不会通知 VTP 域本地配置的 VLAN。配置成透明模式的交换机还是会收到 VTP 配置帧并传递这些帧到所有的骨干端口。这允许 VTP 客户交换机可以连接到一个 VTP 透明交换机。客户交换机通过透明交换机可以和 VTP 服务器交换 VLAN 配置信息。

4）VTP 数据帧

用来配置和维持 VTP 域的数据帧可以封装成 802.1Q 或者 ISL 帧格式（inter switch link，Cisco 公司提出的专用 VLAN 帧格式）。VTP 使用一个保留的广播地址作为所有帧的目的地。这个广播地址 0x01-00-00-0C-CC-CC-CC 伴随着一个子网接入协议（SNAP）的逻辑链路控制（LLC）码，和一个在 SNAP 头的 2003 类型码。每个数据帧包含一个 VTP 头和 VTP 消息类型。有三种类型的 VTP 消息：

- summary（摘要）
- Subset（子集）
- Request（请求）

Summary 帧（摘要帧）：摘要帧可以是 VTP 服务器或者 VTP 客户机发出的，每 5 分钟一次或者当 VTP 域发生改变后立即发出。摘要广播包括 VTP 域的基本信息和配置的修改情况。摘要帧可能跟随着许多的详细的描述帧——子集（subset）帧。

Subset 帧（子集帧）：子集帧用来提供 VTP 域内每个 VLAN 的详细信息。子集帧可以是对 VTP 请求帧的响应，或者当配置改变时发出（和摘要帧一起发出）。

Request 帧（请求帧）：当以下的情况之一发生时，VTP 客户机发送请求帧（request）到 VTP 服务器。

- VTP 域名字改变。
- VTP 客户交换机收到一个配置修改号码更高的摘要广播消息。
- 丢失了一条子集帧。
- 交换机重启。
- VTP 服务器将用一条摘要帧和能够满足请求的若干条子集帧进行响应。

1.6　广域网与接入网

1.6.1　广域网的概念

广域网（WAN）是指将跨地区的各种局域网、计算机、终端等互连在一起的计算机通信网络。目前，常见的广域网有公用电话网、公用分组交换网、公用数字数据网、宽

带综合业务数字网、帧中继网和大量的专用网。

与覆盖范围较小的局域网相比较，广域网具有以下特点：

（1）覆盖范围广，可达数千，甚至数万公里。

（2）使用多种传输介质，例如有线介质有光纤、双绞线、同轴电缆等，无线介质有微波、卫星、红外线、激光等。

（3）数据传输延时大，例如卫星通信的延时可达几秒钟。

（4）广域网管理、维护较困难。

1.6.2 虚电路与数据报实现方法

广域网可以提供面向连接和无连接两种服务模式。对应于两种服务模式，广域网有两种组网方式：虚电路（virtual circuit）方式和数据报（datagram）方式。

1．虚电路

虚电路传输方式中，当源端系统与目的端系统通信时，前者必须先与后者建立一条数据通路。为此，源端发出虚呼叫分组，并按一定路由算法到达目的端。这时便在通信子网中形成一条源/目的节点之间的逻辑通路（虚呼叫分组走过的路径），即虚电路。此后，两端系统的传输实体之间进行的所有通信都在这条虚线路上运行，这与电话系统的工作原理相似。这里要注意的是这条逻辑通路不是专用的，所以称之为“虚”电路。每个节点到其他任一节点之间可能有若干条虚电路支持特定的两个端系统之间的数据传输，两个端系统之间也可以有多条虚电路为不同的进程服务，这些虚电路的实际路径可能相同也可能不同。

在逻辑上我们可以把节点间的物理信道看作由多条逻辑信道所组成，而这些逻辑信道实际上由节点内部的分组缓冲器来实现。所以当我们说占用某条逻辑信道，实质上是指占用了该段物理信道上节点分配的分组缓冲器。不同的逻辑信道在节点内部通过逻辑信道号加以区分，各条逻辑信道异步时复用同一条物理信道。

实际上一条虚电路可能要经过多个中间节点，在节点间的各段物理信道上都要占用一条逻辑信道用以传送分组。由于各节点均独立地为通过的虚电路分配逻辑信道，也即同一条虚电路通过各段信道所获取的逻辑信道可能是不相同的，所以各节点内部必须建立一张虚电路表，用以记录该点的各条虚电路所占用的各个逻辑信道。

为了能使节点区分一个分组属于哪条虚电路，而且同一条虚电路的分组在各段逻辑信道上的逻辑信道号可能也不相同。所以每个分组必须携带一个逻辑信道号；传输中，当一个分组到达节点时，节点根据其携带的逻辑信道号查找虚电路表，以确定该分组应发往的下一个节点及其下一段信道上所占用的逻辑信道号，由该逻辑信道号替换分组中原先的逻辑信道号，再将该分组发往下一个节点。

各节点的虚电路表空间和逻辑信道号都是网络资源，当虚电路拆除时必须回收。这可通过某端系统发出一个拆链请求分组，告知虚电路中各节点删除虚电路表有关表项。

2. 数据报

数据报方式中，源节点与目的节点通信时不必事先与目的节点建立数据通路。通信子网接收源节点送来的数据，经编址、打包后，各自独立的在源节点和目的节点之间寻径传输。在传输过程中，通信子网不负责差错控制，报文到达目的节点的顺序与源节点的发送顺序也不一定相同，有些数据报甚至还可能在途中丢失。因此，采用数据报服务的通信子网，主机的传输层必须具有差错检测和恢复功能，并能对报文进行再排序。这类服务没有建立链路和拆除链路的过程，被称为无连接服务。数据报传送不需要建立虚电路，但网络节点要为每个数据报做路由选择。

3. 两者的比较

数据报与虚电路两种方式各有优缺点，表 1-5 总结了两种方式的不同之处。

表 1-5　数据报与虚电路方式的比较

项 目 类 型	数据报服务	虚电路服务
电路设置	不需要	需要
地址	每个分组都有源端和目的端的地址	每个分组都含有一个虚电路号
状态信息	子网不存储状态信息	建立好的每条虚电路都要求占有虚电路表空间
路由选择	对每个分组独立选择	当虚电路建好后，路由就已确定，所有分组都经过此路由
路由器失败的影响	除了在崩溃时全丢失分组外，无其他影响	所有经过失效路由器的虚电路都要被终止
拥塞控制	难	如果有足够的缓冲区，则容易控制

1.6.3　拥塞控制

1.6.3.1　拥塞概念

当网络中存在过多的数据包时，网络的性能就会下降，这种现象称为拥塞。拥塞是一种持续过载的网络状态，此时用户对网络资源（包括链路带宽、存储空间和处理能力等）的需求超过了其固有的容量。在网络发生拥塞时，会导致吞吐量下降，严重时会发生“拥塞崩溃”（congestion collapse）现象。

1.6.3.2　拥塞控制原理

拥塞发生的根本原因在于用户提供给网络的负载大于网络资源容量和处理能力。其典型表现就是数据包时延增加、丢弃概率增大、上层应用系统性能显著下降等。网络产生拥塞的直接原因主要有以下几个方面：

1）带宽容量相对不足

低速数据链路对于高速数据流的输入会产生拥塞。根据香农信息理论：任何信道带宽最大值为 $C=B\cdot\log_2(1+S/N)$，其中 N 为信道白噪声的平均功率，S 为信源的平均功率，B 为信道带宽。它要求所有信源发送的速率 R 必须小于或等于信道容量 C。如果 R 大于 C，则在网络低速链路处就会形成带宽瓶颈，严重时发生拥塞。

2）队列容量相对不足

为了处理突发流量和流速率的变化，路由器在出口链路前建立了一个队列，它可以接纳一些突发流量，适应网络环境的变化。但是路由器上的存储空间十分有限，它不能无限的加大队列容量，而且加大队列容量还会带来端到端延迟增加等其他问题。

3）路由器的处理能力弱

如果路由器的 CPU 在执行排队缓存、更新路由表等功能时，处理速度跟不上高速链路，也会产生拥塞。

4）网络流量分布不均衡

拥塞总是发生在网络中资源相对短缺的位置。拥塞发生位置的不均衡反应了 Internet 本身的不均衡性。首先是资源分布的不均衡，在网络组建之前并没有经过良好的规划和设计，而是在各种不同容量、不同形式的网络都已经运行起来后才设法将它们统一连接起来，这样就必然大量存在网络带宽分布不均的情况。其次是网络流量的不均衡，在不同时刻，各种需求往往导致某些节点上的资源受到大量的访问，而大量存在的客户服务器模式也加剧了流量分布不均的产生。

随着网络不断成熟与发展，网络内部带宽容量和队列资源不足的问题已经逐渐好转，但流量分布不均衡的问题则是无法完全解决的。

拥塞虽然是由于网络资源的稀缺引起的，但单纯增加资源并不能避免拥塞的发生。例如增加缓存空间到一定程度时，只会加重拥塞，而不是减轻拥塞，这是因为当数据包经过长时间排队完成转发时，它们很可能早已超时，从而引起源端超时重发，而这些数据包还会继续传输到下一路由器，从而浪费网络资源，加重网络拥塞。事实上，缓存空间不足导致的丢包更多的是拥塞的“症状”而非原因。另外，增加链路带宽及提高处理能力也不能解决拥塞问题。

拥塞本身是一个动态问题，它不可能只靠静态的方案来解决，而需要协议能够在网络出现拥塞时保护网络的正常运行。目前对互联网进行的拥塞控制主要是依靠在源端执行的基于窗口的 TCP 拥塞控制机制。网络本身对拥塞控制所起的作用较小，但近几年这方面的研究已经成了一个新的热点。

从控制理论的角度，拥塞控制算法可以分为开环控制和闭环控制两大类。当流量特征可以准确规定、性能要求可以事先获得时，适于使用开环控制；当流量特征不能准确描述或者当系统不提供资源预留时，适于使用闭环控制。Internet 中主要采用闭环控制方式，以动态适应网络的变化，其设计关键是如何生成反馈信息和如何对反馈信息进行响应。

闭环的拥塞控制分为三个阶段：检测网络中拥塞的发生；将拥塞信息报告到拥塞控制点；拥塞控制点根据拥塞信息进行调整以消除拥塞。闭环的拥塞控制可以动态的适应网络的变化，但算法性能受到反馈延迟的严重影响。当拥塞发生点和控制点之间的延迟很大时，算法性能会严重下降。

1.6.3.3　拥塞控制方法

从拥塞控制方法施行的位置来分，可以分为基于终端的拥塞控制和基于链路（路由器）的拥塞控制。链路方法在网络设备（如路由器和交换机）中执行，作用是检测网络拥塞的发生，产生拥塞反馈信息。终端方法在主机和网络边缘设备中执行，作用是根据反馈信息调整发送速率。拥塞控制算法设计的关键问题是如何生成反馈信息和如何对反馈信息进行响应。

1．拥塞控制的链路方法

拥塞控制的链路方法假定网络传输流的端设备对丢包和标记做出响应，并调整自身的吞吐量，这种假设是与 TCP 的拥塞控制相对应的。

传统网络设备采用 PQM（被动队列管理）来管理网络中间节点数据包的排队，它采用 FIFO 的 Drop-tail 丢包策略，仅在输入队列溢出时进行丢包，这种方式容易产生 Lock-out（锁外），Full-queues（满列）和 Global synchronization（全局同步）等问题。虽然采用 Random-drop 和 Drop-front 丢包策略可以避免 Lock-out 问题，但是却无法解决满队列和全局同步引起的振荡问题。

为了缓解上面提到的这些问题，出现了 AQM（主动队列管理）技术。AQM 是路由器在队列充满之前丢包，这样端节点便能在队列溢出前对拥塞做出反应，从而达到避免拥塞的目的。以 AQM 技术为基础又进一步提出了一些改进和优化方法。

2．拥塞控制的终端方法

1）TCP 拥塞控制

使用最广泛的基于终端的拥塞控制方法是 TCP 协议的拥塞控制算法。TCP 是目前在互联网中使用最广泛的传输协议。广义的来讲，TCP 拥塞控制的概念是每个源端判断当前网络中有多少可用容量，从而知道它可以安全完成传送的分组数。一旦某个源端有这么多分组在传送，它用确认（ACK）信号的到达表明它有一个分组已经离开网络，因而它不需要增加拥塞级别就可以安全地向网络中发送一个新的分组，通过使用确认信息来协调分组的传送，TCP 称为自同步（self-clocking）的。

TCP 拥塞控制机制包括慢启动（slow start）、拥塞避免、快速重传（fast retransmit）、快速恢复（fast recovery）、选择性应答（SACK）等。通过在终端上对网络的拥塞情况做出适当的调整，可以大大提高网络传输的性能，减少拥塞发生的可能性。

TCP 中使用的拥塞控制算法已经成为保证目前互联网稳定性的重要因素。

2）ECN（Explicit Congestion Notification）

由于目前 TCP 使用丢包作为隐式的拥塞指示信号，即发送方检测到重复的 ACK 或者重传超时的时候认为发生拥塞，这种机制在用于检测拥塞时开销较大，需要等待较长的周期才能发现拥塞，降低了拥塞控制的效率。为此，显示拥塞通告算法 ECN 可以减少由于不必要的丢包产生的延时。其主要思想是通过路由器对拥塞的判断，显示的设置拥塞标记，发送端主机通过网络中返回的带拥塞反馈标记的包发现拥塞。

3）XCP 和 VCP

随着互联网的发展，端到端带宽时延积逐渐增大，传统的 TCP 算法逐渐暴露出它的问题。TCP 的加式增加相对于网络带宽显得过于缓慢，往往不能充分地利用链路资源，因此，不少算法都针对大带宽时延积网络提出 MIMD（积式增加积式减少），提高慢启动速度等方案，这些算法一方面针对大带宽时延积网络做出了优化，但另一方面也失去了对小带宽时延积网络的适应性。

针对这些问题，提出了一种新的互联网拥塞控制机制 XCP。XCP（eXplicit Control Protocol）事实上是对 ECN 机制的一种扩充，它的主要思想是充分利用网络中间节点对链路带宽的认知，为端到端拥塞控制机制提供比是否发生拥塞更多和更有效的网络带宽提示，从而使控制机制能够更快的适应当前的网络状况。

VCP（Variable-structure congestion Control Protocol）协议是一个新的传输协议。该算法可以认为是在 ECN 和 XCP 算法的基础上发展而来，它继承了 ECN 和 XCP 利用路由器提供拥塞指示的思想，但它试图避免大幅度修改传统 TCP＋AQM/ECN 网络的主要结构，利用现有的 ECNbit 达到与 XCP 类似的性能。

1.6.4 公用网

广域网与局域网在构建方面的主要差别是广域网必须借助公共通信网络（公用网）。目前，提供公用网的主要是电信部门。公用网的种类比较多，基本上可以分为三大类：一类是电路交换网，一类是分组交换网，另外还有一些属于专用线路连接的通信网。

1.6.4.1 ISDN/BISDN 网络

1．ISDN 及其特点

综合业务数字网（Integrated Service Digital Network，ISDN），它是在现有电话网的基础上发展起来的，用单一网络提供不同类型的业务，实现完全的开放系统互连和通信。ISDN 将分组交换能力、电路交换能力及无交换能力都包含在其内部，具有业务综合、端到端的数字连接、标准接口特性。用户通过 ISDN 网络既能进行高速数据传输（64Kbps～622Mbps）和图像传送，又能进行语音传送，并且比电话网和数据网更为有效、经济和方便。

ISDN 与 PSTN（公共电话交换网）相比具有以下两个特点：

（1）ISDN 的端到端使用全数字式信道。

（2）ISDN 的用户只需要通过一组标准的多用途接口就能进网。

虽然 ISDN 尚未如最初愿望的那样获得广泛的应用，但其技术却已经历了两代。

第一代 ISDN 称为窄带 ISDN（N-ISDN）。它利用 64Kbps 的信道作为基本交换单位，采用电路交换技术。

第二代 ISDN 称为宽带 ISDN（B-ISDN）。它支持更高的数据传输速率，发展趋势是采用报文分组交换技术。

目前 N-ISDN 定义了两类用户访问速率：基本访问速率和基群访问速率。

1）基本访问速率（basic access rate）

基本访问速率由两个速率为 64Kbps 的 B 信道和 1 个速率为 16Kbps 的 D 信道组成（2B+D）。B 信道用于传送用户数据；D 信道用于传送控制信息；加上分帧、同步等其他开销，总速率为 192Kbps。

2）基群访问速率（primary access rate）

基群访问速率可由多种信道混合而成。在北美和日本使用（23B+D）的结构，速率为 1.544Mbps；而在欧洲则使用（30B+D）的结构，其中 B、D 信道均为 64Kbps。

基本访问速率可利用现有用户电话线支持，提供电话、传真等常规业务。基群访问速率则是针对专用小型电话交换机（PBX）或 LAN 等业务量大的单位用户。

2．ISDN 的结构

ISDN 的基本结构如图 1-60 所示，由该图可以看出，ISDN 包括用户-网络接口、网络功能和 ISDN 的信令系统。

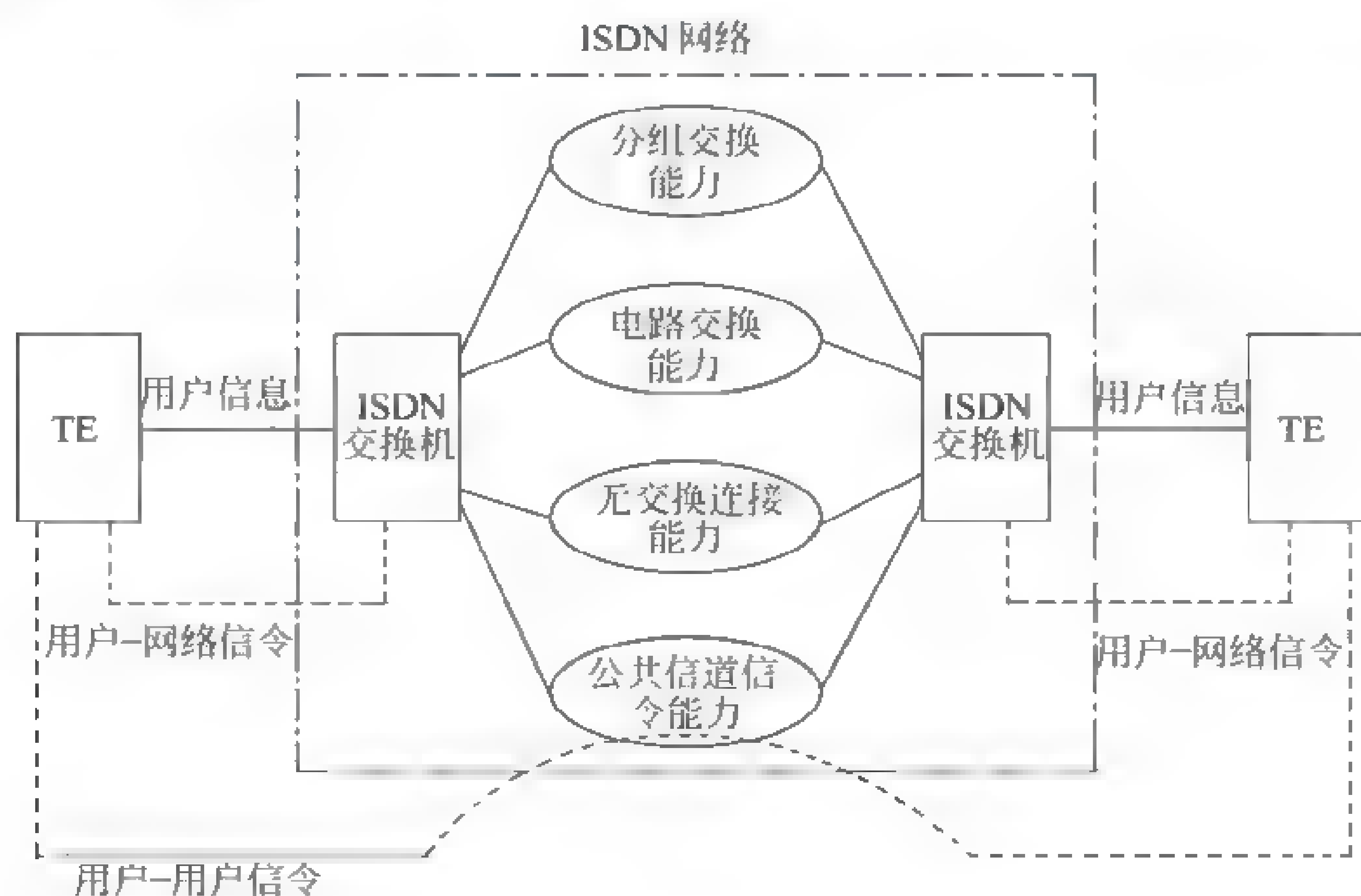


图 1-60　ISDN 结构图

1）ISDN 用户-网络接口

ISDN 用户 网络接口的作用是使用户终端与 ISDN 网络之间或网络与用户之间能够相互交换信息，该接口主要具有以下功能：

（1）具有利用同一接口提供多种业务的能力。

根据用户需求，在呼叫的基础上，选择信息的比特速率、交换方式或编码方式等。

（2）具有多终端配置功能。

多个终端可以连接在同一个接口上，允许同时使用这些不同的终端。

（3）具有终端的移动性。

利用标准插座，使终端能够在通信过程中移动和重新恢复通信的连接。

（4）在主叫用户和被叫用户终端之间进行兼容性检查。

为了检验主叫与被叫终端能够相互通信，例如保证电话与电话终端、传真与传真终端等高层的一致性，需要具有兼容性检验的功能。

2）ISDN 的网络功能

ISDN 网络具有多种能力，包括电路交换能力、分组交换能力、无交换连接能力和公共信道信令能力。在一般情况下，网络只提供低层（OSI 模型 1～3 层）功能。

3）ISDN 的信令系统

ISDN 具有三种不同的信令：用户-网络信令、网络内部信令和用户-用户信令。这三种信令的工作范围不同：用户-网络信令是用户终端设备和网络之间的控制信号；网络内部信令是交换机之间的控制信号；用户-用户信令则透明地穿过网络，在用户之间传送，是用户终端设备之间的控制信号。ISDN 的全部信令都采用公共信道信令。

3．B-ISDN 网

随着用户信息传送量和传送速率的不断提高，N-ISDN 已无法满足用户要求。例如，要传送高清晰度电视图像要求达到 155Mbps 量级的速率，要支持多个交互式或分布式应用，一个用户线的总容量需求可能达到 622Mbps 的数量级。在此情况下，人们提出了宽带 ISDN，即 B-ISDN。所谓宽带是指要求传送信道能够支持大于基群数量的服务。B-ISDN 可以提供视频点播（VOD）、电视会议、高速局域网互联以及高速数据传输等业务。采用 B-ISDN 名称旨在强调 ISDN 的宽带特性，而实际上它应该支持宽带和其他 ISDN 业务。B-ISDN 提出后，为区别起见，人们将原来的 ISDN 称为 N-ISDN。

B-ISDN 要支持高速率，要处理很广范围内各种不同速率和传输质量的需求，需要面临两大技术问题：一是高速传输；二是高速交换。光纤通信技术已经给前者提供了良好的支持；而异步传输模式（Asynchronous Transfer Mode，ATM）为实现高速交换展示了好的前景。近年来电路交换设备的功能日益增强且越来越多地采用光纤干线，但利用电路交换技术难以圆满解决 B-ISDN 对不同速率和不同传输质量控制的需求。而 ATM 技术可以满足 B-ISDN 的此需求。正因为这样，ATM 和 SONET 技术与 B-ISDN 结下了不解之缘。光交换技术和 ATM 技术成为实现 B-ISDN 的主要技术。

1.6.4.2　DDN 网络

数字数据网（Digital Data Network，DDN）是一种利用数字信道提供数据通信的传输网，它主要提供点到点及点到多点的数字专线或专网。

DDN 由数字通道、DDN 节点、网管系统和用户环路组成。DDN 的传输介质主要有光纤、数字微波、卫星信道等。DDN 采用了计算机管理的数字交叉连接（Data Cross Connection，DXC）技术，为用户提供半永久性连接电路，即 DDN 提供的信道是非交换、用户独占的永久虚电路（PVC）。一旦用户提出申请，网络管理员便可以通过软件命令改变用户专线的路由或专网结构，而无须经过物理线路的改造扩建工程。因此 DDN 极易根据用户的需要，在约定的时间内接通所需带宽的线路。

DDN 为用户提供的基本业务是点到点的专线。从用户角度来看，租用一条点到点的专线就是租用了一条高质量、高带宽的数字信道。用户在 DDN 上租用一条点到点数字专线与租用一条电话专线十分类似。DDN 专线与电话专线的区别在于：电话专线是固定的物理连接，而且电话专线是模拟信道，带宽窄、质量差、数据传输率低；而 DDN 专线是半固定连接，其数据传输率和路由可随时根据需要申请改变。另外，DDN 专线是数字信道，其质量高、带宽宽，并且采用热冗余技术，具有路由故障自动迂回功能。

1.6.4.3　SDH 网络

SDH（Synchronous Digital Hierarchy，光同步数字传输网）最初由美国贝尔通信研究所提出，采用了一整套分等级的校准数字传递结构组成的同步网络（SONET）。后来国际电报电话咨询委员会（CCITT）接受了这个概念并重新命名为同步数字体系（SDH），使之成为不仅适用于光纤也适用于微波和卫星传输的通用技术体制。SDH 网是一种全新技术体制，具有路由自动选择能力，上下电路维护、控制、管理功能强，标准统一，便于传输更高速率的业务等优点。该网的推出使电视、图像、话音、数据以及数字微波传输发生了重大改变。SDH 网络的引入和使用，就可以比较容易地实现高智能的、高效的、维护功能齐全、操作运行廉价的信息高速公路。因此，在 SDH 技术推出的短时间内，其产品和应用就得到了极为迅猛的发展。

SDH 网络具有以下主要特点。

1）统一的光接口

SDH 网络对同步数字系统光接口有统一规定，包括一系列光接口详细参数及其测量方法。如光发射机的平均发射光功率范围、最小消光比、信号眼图模板、光源的光谱特性、光通路允许衰耗、色散值和反射、接收机灵敏度、动态范围等。

2）自愈环

自愈环的作用是提高网络的生存性，即在无人参与的情况下，网络能及时地发现错误，并能在极短的时间内自动恢复承载的业务，而用户根本感觉不到网络的故障。自愈

环的结构有许多种，主要有路由保护、二纤单向环、二纤双向环和利用 DXC 保护的自愈环。

3）SDH 网同步

SDH 网同步结构采用主从同步方式，要求所有网络单元时钟都能最终跟踪到全网的基准主时钟。局内同步分配一般用星型拓扑，即局内所有时钟由本局最高质量的时钟获取定时，只有高质量的时钟由外部定时同步。获取的定时由 SDH 网络单元经同步链路送往其他局的网络单元。由于 TU（支路单元）指针调整引起的抖动会影响时钟性能，因而不再推荐在 TU 内传送的一次群信号作为局间同步分配，而直接用 STM-N 传送同步信息。局间同步分配一般采用树型拓扑。标准的 SDH 传输系统中一般带有公务电话功能，以方便远距离环网节点间设备的调试和维护，传统设备中公务电话位于光群路接口模块上，这样只要光群路能正常工作，即可实现节点间的电话对讲。

1.6.4.4 WDM 网络

1．WDM 技术

全球网络用户的大量增长和大容量业务的发展，使得带宽需求量成线性增长，如何有效地增加骨干网的传输能力成为众多 ISP（Internet Service Provider，服务提供商）必须面对的重要问题。虽然目前的骨干网多数已使用光纤链路来传输数据，但是传统的 SDH/SONET（Synchronous Digital Hierarchy/Synchronous Optical Network）技术只能以特定的传输速率（如 2.5Gbps）在光纤中的单个波长通道上传输数据，单纯依靠增加单波长传输速率的方法，例如使用更高速的 TDM（Time Division Multiplexing，时分复用）技术，将碰到诸如因传输速率逼近电层处理极限而使设备成本迅速增加等问题。然而，一根光纤可提供的理论传输带宽约为 50THz，可见光纤的容量还远远没有得到充分利用。WDM（Wavelength Division Multiplexing，波分复用）技术可以充分利用光纤的低损耗带宽，在一根光纤中的不同波长上异步、高速传输各种格式的信号，是挖掘光纤巨大带宽资源的最佳技术。

波分复用（WDM）实质是光域上的 FDM（Frequency Division Multiplexing，频分复用）技术，每个波长通路通过频域的分割实现，每个波长通路占用一段光纤的带宽。WDM 技术使用独立的电比特流调制各自的光载波，经复用后在同一根光纤上传送。由于它们的光谱成分不同，在大气传输中是各不干扰的。在接收端使用解复用器（等效于光通带滤波器）将各种载波上的光信号分开。

WDM 技术在光传输网中的典型应用如图 1-61 所示。WDM 系统由光合波器（光复用器）和可以提取独立光波长的光分波器（光解复用器）组成。发射端的发射机发出光波长不同且精度和稳定度能满足一定要求的光信号，经过光合波器、掺铒光纤放大器，送入光纤中传输（光纤线路中可根据需要设置光线路放大器）。到达接收端后，经光纤前置放大器放大，通过光分波器恢复成原来的各路光信号。

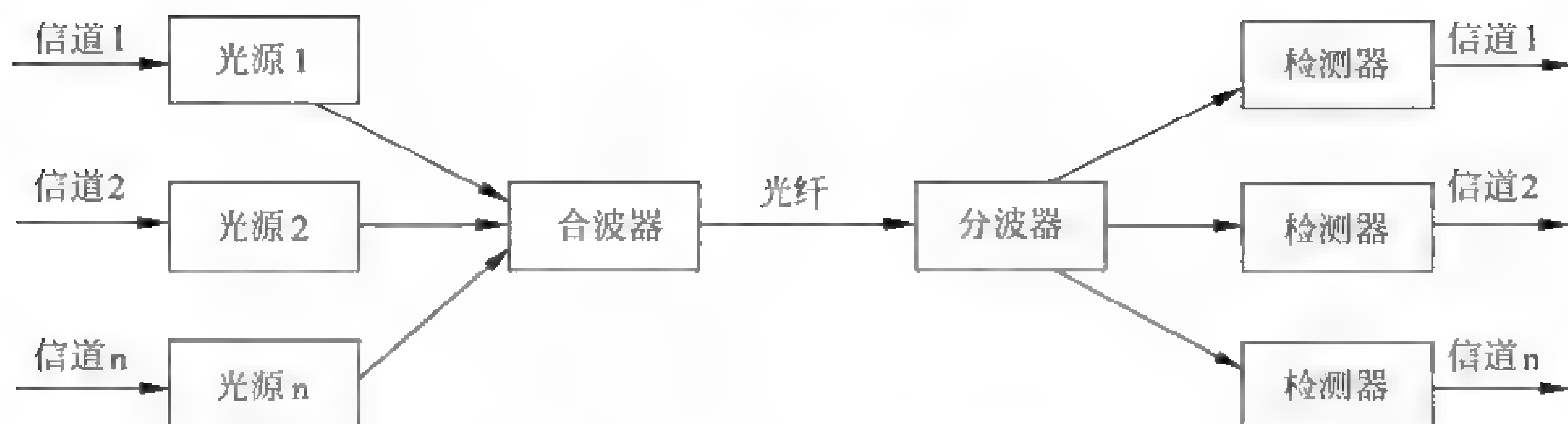


图 1-61　WDM 波分复用系统

WDM 使单波长传输变成多波长同时传输，从而可以大大增加光纤的传输容量。例如，如果每个波长的传输速率为 2.5Gbps，在一根光纤中同时使用 4 个波长，则光纤总的传输容量就可达到 2.5×4 =10Gbps。一根光纤可以传输几百个甚至几千个信道，因此，WDM 技术可以充分利用光纤的巨大带宽资源（多于 50THz 的理论可用带宽），使一根光纤的传输容量比单波长传输时的容量增加几倍、几十倍甚至几百倍，可以认为 WDM 技术将为光传输网的发展提供几乎取之不尽的资源。

2．WDM 技术特点

WDM 技术具有下述特点：

（1）传输容量大，可节约宝贵的光纤资源。对单波长光纤系统而言，收发一个信号需要使用一对光纤，而对于 WDM 系统，不管有多少个信号，整个复用系统只需要一对光纤。

（2）对各类业务信号“透明”，可以传输不同类型的信号，如数字信号、模拟信号等，并能对其进行合成和分解。

（3）网络扩容时不需要敷设更多的光纤，也不需要使用高速的网络部件，只需要换端机和增加一个附加光波长就可以引入任意新业务或扩充容量，因此 WDM 技术是理想的扩容手段。

（4）组建动态可重构的光网络，在网络节点使用光分插复用器（OADM）或者使用光交叉连接设备（OXC），可以组成具有高度灵活性、高可靠性、高生存性的全光网络。

正是因为 WDM 技术的上述特点，使其在近几年得到了迅猛的发展，并且随着研究的不断深入，WDM 技术将更广泛地应用于未来超高速的传输网络中。

3．WDM 网络结构与节点设备

如图 1-62 所示，现有的传输网络由接入网络和 WDM 核心网络两部分组成。其中具有 WDM 接口的边缘节点构成了接入网络；而由 OXC 波长路由核心节点通过光纤互连而成为 WDM 核心网络。边缘节点具有汇聚业务量的功能，因此需要能汇聚各种小粒度业务量的电处理设备，来实现业务汇聚。核心网中的 OXC 节点具有多个标准的光纤接口，可对任一光纤信号或其波长信号与其他光纤信号进行可控的连接，它可能具有波长

转换能力，不过只能以波长级的粒度交换业务。通常 WDM 网络结构指的就是 WDM 核心网络这部分。

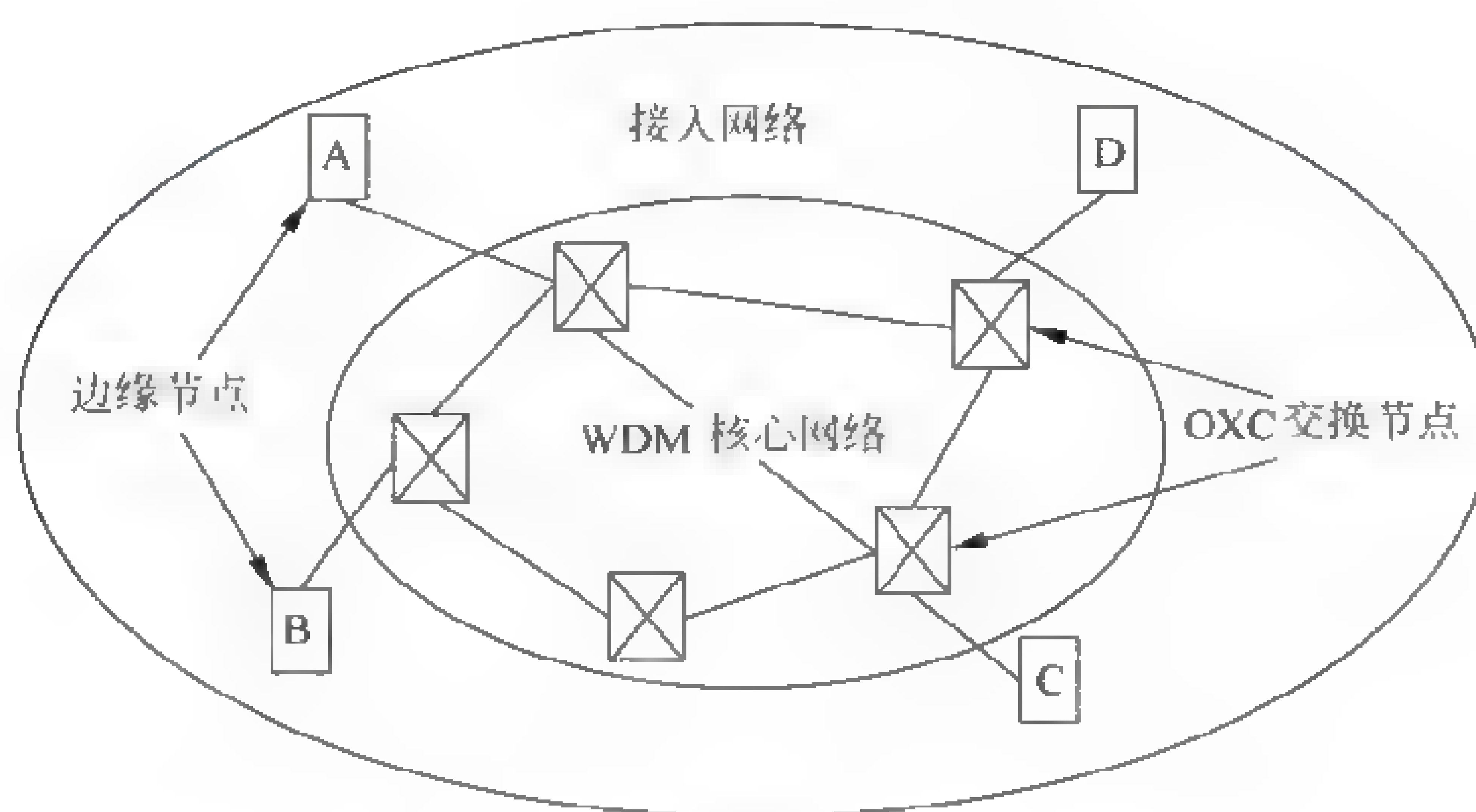


图 1-62 接入网络和 WDM 核心网络

WDM 网络中的节点 OADM 和 OXC 设备，通常由 WDM 复用/解复用器、光交换矩阵（由光开关和控制部分组成）、波长转换器和节点管理系统组成，主要完成光路上下、光层的带宽管理、光网络的保护、恢复和动态重构等功能。

1.6.4.5 MSTP 网络

1. MSTP 技术

MSTP（Multi-Service Transport Platform，基于 SDH 的多业务传送平台）是指基于 SDH 平台同时实现 TDM、ATM、以太网等业务的接入、处理和传送，提供统一网管的多业务节点。基于 SDH 的多业务传送节点除应具有标准 SDH 传送节点所具有的功能外，还具有以下主要功能特征：

（1）具有 TDM 业务、ATM 业务或以太网业务的接入功能。

（2）具有 TDM 业务、ATM 业务或以太网业务的传送功能，包括点到点的透明传送功能。

（3）具有 ATM 业务或以太网业务的带宽统计复用功能。

（4）具有 ATM 业务或以太网业务映射到 SDH 虚容器的指配功能。

基于 SDH 的多业务传送节点可根据网络需求应用在传送网的接入层、汇聚层，应用在骨干层的情况有待研究。

2. MSTP 的工作原理

MSTP 是将传统的 SDH 复用器、数字交叉连接器（DXC）、WDM 终端、网络二层交换机和 IP 边缘路由器等多个独立的设备集成为一个网络设备，即基于 SDH 技术的多

业务传送平台（MSTP），进行统一控制和管理。基于 SDH 的 MSTP 最适合作为网络边缘的融合节点支持混合型业务，特别是以 TDM 业务为主的混合业务。它不仅适合缺乏网络基础设施的新运营商，应用于局间或 POP 间，还适合于大企事业用户驻地。而且即便对于已铺设了大量 SDH 网的运营公司，以 SDH 为基础的多业务平台可以更有效地支持分组数据业务，有助于实现从电路交换网向分组网的过渡。所以，它将成为城域网近期的主流技术之一。

这就要求 SDH 必须从传送网转变为传送网和业务网一体化的多业务平台，即融合的多业务节点。MSTP 的实现基础是充分利用 SDH 技术对传输业务数据流提供保护恢复能力和较小的延时性能，并对网络业务支撑层加以改造，以适应多业务应用，实现对二层、三层的数据智能支持。即将传送节点与各种业务节点融合在一起，构成业务层和传送层一体化的 SDH 业务节点，称为融合的网络节点或多业务节点，主要定位于网络边缘。

3. MSTP 的特点

（1）业务的带宽灵活配置，MSTP 上提供的 10/100/1000Mbps 系列接口，通过 VC 的捆绑可以满足各种用户的需求。

（2）可以根据业务的需要，工作在端口组方式和 VLAN 方式。

① 端口组方式。

单板上全部的系统和用户端口均在一个端口组内。这种方式只能应用于点对点对开的业务。换句话说，也就是任何一个用户端口和任何一个系统端口（因为只有一个方向，所以没有必要启动所有的系统端口，一个就足够了）被启用了，网线插在任何一个启用的用户端口上，那个用户端口就享有了所有带宽，业务就可以开通。

② VLAN 方式。

VLAN 方式分为接入模式和干线模式。

其中的接入模式，如果不设定 VLAN ID，则端口处于端口组的工作方式下，单板上全部的系统和用户端口均在一个端口组内。

如果设定了 VLAN ID，需要设定“端口 VLAN 标记”。这是因为交换芯片会为收到的数据包增加 VLAN ID，然后通过系统端口走光纤发到对端同样 VLAN ID 的端口上。比如某个用户端口 VLAN ID 为 2，则对应站点的用户端口的 VLAN ID 也应该设定为 2。这种模式可以应用于多个方向的 MSTP 业务，这时每个方向的端口都要设置不同的 VLAN ID。然后把该方向的用户端口和系统端口放置到一个虚拟网桥中（该虚拟网桥的 VLAN ID 必须与“端口 VLAN 标记”一样）。

（3）可以工作在全双工、半双工和自适应模式下，具备 MAC 地址自学习功能。

（4）QoS 设置。

QoS 实际上限制端口的发送，原理是发送端口根据业务优先级上有许多发送队列，根据 QoS 的配置和一定的算法完成各类优先级业务的发送。因此，当一个端口可能发送来自多个来源的业务，而且总的流量可能超过发送端口的发送带宽时，可以设置端口的

QoS 能力，并相应地设置各种业务的优先级配置。当 QoS 不作配置时，带宽平均分配，多个来源的业务尽力传输。QoS 的配置就是规定各端口在共享同一带宽时的优先级及所占用带宽的额度。

（5）对每个客户独立运行生成树协议。

1.6.4.6 移动通信网络

移动通信网络目前正从第二代向第三代（简称 3G）演进。第二代移动通信网络主要有 GSM、GPRS 和 CDMA 等；而 3G 网络依据三大主流无线接入技术有 WCDMA、CDMA2000 和 TD-SCDMA 网络。

1．GSM 网络

GSM（Global System for Mobile Communication，全球移动通信系统）规范的第一阶段于 1989 年完成，第一个系统于 1991 年建成，自 1992 年商业业务运营开始，目前 100 多个国家的 GMS 用户已经有了世界范围的漫游覆盖、各种操作环境下出色的话音质量及许多增值业务。移动数据通信是在数据通信基础上发展起来的一种通信方式。以往的数据通信依赖于有线传输，因此只适合于固定终端或计算机之间的通信，而移动数据通信是通过无线电波来传送数据的，因而有可能实现移动状态下的数据通信。狭义地说，移动数据通信就是计算机间或计算机与人之间的无线通信，它通过与有线数据网互连，把有线数据网络的应用扩展到移动和便携用户。

GSM 移动数据业务主要分为电路型数据业务和分组数据业务。GSM 第一阶段提供的 9600bps 传输速率数据业务和短消息业务及 Phase 2+阶段提出的 HSCSD 都属于电路型数据业务。Phase 2+阶段提出的 GPRS（General Packet Radio Service，通用分组无线业务）则属于分组型数据业务，是建立在 GSM 基础上的 2.5G 的无线网络技术，是第二代移动通信技术 GSM 向第三代移动通信（3G）的过渡技术，面向用户提供移动分组的 IP 或者 X.25 连接。由于引入分组概念，GPRS 为目前使用的设备无线接入 Internet 提供了一种先进的有效的手段，可应用于移动计算、手持设备的 Internet 互联、远程数据采集和监控等多种场合。

2．GPRS 网络

GPRS 是一种采用分组交换技术传输数据及信令的高效率数据传输方式。GPRS 是区别于原有 GSM 电路交换方式的另一种数据传输方式，它利用存储转发原理，把不同终端的数据分割成等长标准数据格式，通过非专用的逻辑子信道进行数据快速交换，即将信息分成数据分组或信息包，再加上包含目的地址、分组编号、控制比特等的分组头，沿不同路由进行传送，接收端按照分组编号重新组装成原始信息。分组通信的实质是依靠高处理能力的计算机来充分利用宝贵的通信信道资源。基于分组交换的 GPRS 业务理论上的速率可达到 171.2kbps。

分组交换基本上不是实时系统，延时也不固定，但可以使不同的数据传输“共用”

传输带宽；有数据时占用带宽，无数据时不占用，从而分享资源。在 GSM 无线系统中，无线信道资源非常宝贵。如采用电路交换，通信需要建立端到端的连接，信道只能被一个用户独占，在成本效率上显然缺乏可行性。而采用分组交换的 GPRS 则可灵活运用无线信道，每一个用户可以有多个无线信道，而同一信道又可以由几个用户共享，从而极大的提高了无线资源的利用率。由于 GPRS 用户的数据通信费是以数据流量为基础，而不考虑通信时长，所以 GPRS 用于 IP 业务的接入将更为用户所接受。

3．CDMA 网络

目前的数字移动通信网的主要多址方式是 TDMA。TDMA 系统（GSM，DAMPS）在频谱效率上约是模拟系统的 3 倍，容量有限；在话音质量上 13kbps 编码也很难达到有线电话水平。TDMA 系统的业务综合能力较高，能进行数据和话音的综合，但终端接入速率有限（最高 9.6kbps）；TDMA 系统无软切换功能，因而容易掉话，影响服务质量；TDMA 系统的国际漫游协议还有待进一步的完善和开发。因而 TDMA 并不是现代蜂窝移动通信的最佳无线接入，而 CDMA 多址技术完全适合现代移动通信网所要求的大容量、高质量、综合业务、软切换、国际漫游等。

CDMA 多址技术的原理是基于扩频技术，即将需传送的具有一定信号带宽信息数据，用一个带宽远大于信号带宽的高速伪随机码进行调制，使原数据信号的带宽被扩展，再通过载波调制并发送出去。接收端使用完全相同的伪随机码，与接收的宽带信号作相关处理，把宽带信号换成包含原信息数据的窄带信号即解扩，以实现信息的传输。

CDMA 系统本身所固有的许多特点：频率规划简单、系统容量大、频率复用系数高、抗多径能力强、通信质量好、软容量、软切换等，使得它非常适合于数字蜂窝移动通信系统。但是 CDMA 技术也面临着一些问题，除了多径衰落、时延扩展和远近效应等蜂窝移动通信系统所固有的问题以外，也存在着自己所特有的一些问题，比如多址干扰和使用的体制问题等。

4．TD-SCDMA 网络

TD-SCDMA 作为中国提出的第三代移动通信标准（简称3G），自 1998 年正式向ITU（国际电联）提交以来，已完成了标准的专家组评估、ITU 认可并发布、与3GPP（第三代伙伴项目）体系的融合、新技术特性的引入等一系列的国际标准化工作，从而使 TD-SCDMA 标准成为第一个由中国提出的、以我国知识产权为主的、被国际上广泛接受和认可的无线通信国际标准。这是我国电信史上重要的里程碑。

TD-SCDMA 是世界上第一个采用时分双工（TDD）方式和智能天线技术的公众陆地移动通信系统，也是唯一采用同步 CDMA（SCDMA）技术和低码片速率（LCR）的第三代移动通信系统。同时采用了联合检测、软件无线电、接力切换等一系列高新技术。至今为止，其他公众陆地移动通信系统中都没有使用这些技术，TD-SCDMA 系统可以采用这些技术并能保证它们很好的工作。

TD-SCDMA 综合了 TDD 和 CDMA 的所有技术优势，具有灵活的空中接口，并采

用了智能天线、联合检测等先进技术，具有相当高的技术先进性，并且在目前主流标准中具有最高的频谱效率。随着大范围覆盖和高速移动等问题的逐步解决，TD-SCDMA 将成为使用经济并能得到令人满意效果的第三代移动通信解决方案。

1.6.4.7 WiMAX 网络

1. WiMAX 技术

WiMAX（Worldwide Interoperability for Microwave Access）是基于 IEEE 802.16 标准。802.16 是 IEEE-SA 在 1999 年成立的专门开发宽带固定无线技术标准，目标就是要建立一个全球统一的宽带无线接入标准。而 WiMAX 组织也是为了实现这一目标而由几家世界知名企业发起成立的。随着 WiMAX 组织的发展壮大，加快了 802.16 标准的发展，特别是移动 WiMAX-802.16e 标准的提出更加引人注意。

IEEE802.16 标准又称为 IEEE Wireless MAN 空中接口标准，是工作于 2～66GHz 无线频带的空中接口规范。由于它所规定的无线系统覆盖范围可高达 50km，因此 802.16 系统主要应用于城域网，符合该标准的无线接入系统被视为可与 DSL 竞争的最后一公里宽带接入解决方案。根据使用频带高低的不同，802.16 系统可分为应用于视距和非视距两种，其中使用 2～11GHz 频带的系统应用于非视距（NLOS）范围，而使用 10～66GHz 频带的系统应用于视距（LOS）范围。根据是否支持移动特性，802.16 标准又可分为固定宽带无线接入空中接口标准和移动宽带无线接入空中接口标准。

当前，在 IEEE 802.16 协议中规定 WiMAX 支持的业务类型和使用无线信道频率如表 1-6 所示。

表 1-6 IEEE 802.16 的工作频率

空中接口标准	工 作 频 段	支 持 业 务
IEEE 802.16	2～66GHz	固定宽带无线接入
IEEE 802.16a	2～11GHz	固定宽带无线接入
IEEE 802.16c	10～66GHz	固定宽带无线接入的兼容性
IEEE 802.16d	2～66GHz	固定宽带无线接入的修订
IEEE 802.16e	<11GHz	移动宽带无线接入

而现在 WiMAX 网络的相关标准也在不断发展，IEEE 802.16 标准系列到目前为止包括 802.16、802.16a、802.16c、802.16d、802.16e、802.16f 和 802.16g 七个标准，各标准相对应的技术领域如表 1-7 所示。

表 1-7 IEEE 802.16 系列各标准相对应的技术领域

标 准 号	相对应的技术领域
IEEE 802.16	10～66GHz 固定宽带无线接入系统空中接口
IEEE 802.16a	2～11GHz 固定宽带接入系统空中接口
IEEE 802.16c	10～66GHz 固定宽带接入系统的兼容性

续表

标　准　号	相对应的技术领域
IEEE 802.16d	2～66GHz 固定宽带接入系统空中接口
IEEE 802.16e	2～6GHz 固定和移动宽带无线接入系统空中接口管理信息库
IEEE 802.16f	固定宽带无线接入系统空中接口管理信息库（MIB）要求
IEEE 802.16g	固定和移动宽带无线接入系统空中接口管理平面流程和服务

2．802.16 标准的网络结构

图 1-63 所示的为 WiMAX 网络体系结构。

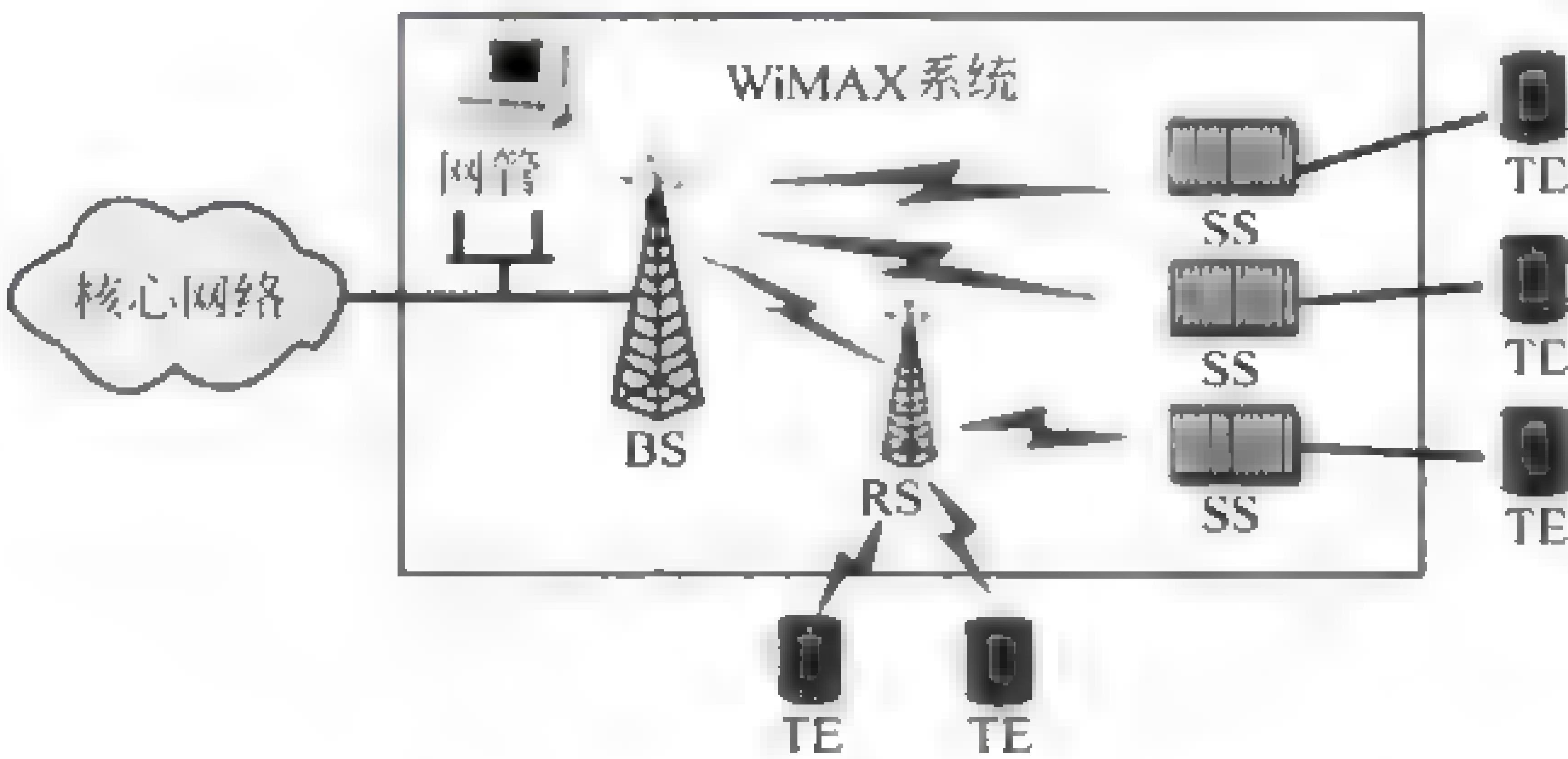


图 1-63　WiMAX 网络结构示意图

WiMAX 网络体系结构包括核心网络、基站（BS）、用户基站（SS）、接力站（RS）、用户终端设备（TE）以及网管。

WiMAX 连接的核心网络通常为传统交换网或 Internet。WiMAX 系统提供核心网与基站之间的接口，但 WiMAX 系统不包括核心网络。

基站提供用户基站与核心网之间的连接，通常采用扇形、定向或全向天线。WiMAX 基站可提供灵活的子信道部署与配置功能，能够使运营商根据所拥有的频段资源灵活规划信道带宽，并根据用户群体情况不断的升级扩展网络。

用户基站提供基站与用户终端设备之间的中继连接。IEEE 802.16 用户基站通常采用固定天线，并被安装在屋顶上。基站与用户基站间采用动态适应信号调制模式，这种模式使得基站根据信号强弱调整到每个用户基站的带宽，以确保与用户基站的正常连接。

接力站通常用于提高基站的覆盖能力，也就是充当一个基站和若干个用户基站（或用户终端设备）间信息的中继站。接力站面向用户侧的下行频率可以与其面向基站的上行频率相同，也可以不同。

WiMAX 系统定义用户终端设备与用户基站间的连接接口，提供用户终端设备的接入。

网管系统用于监视和控制网络内所有的基站和用户基站，提供查询、状态监控、软

件下载、系统参数配置等功能。

在 IEEE 802.16d 及以前的版本中，WiMAX 系统不支持终端设备的移动性，一幢大楼安装一个 SS，起到了固定无线宽带接入的作用。802.16e 协议使网络终端具有移动性，终端设备能够在 BS 之间自由地进行切换和漫游。WiMAX 系统的 MAC 层支持两种网络模式：点到多点（Point to MultiPoint，PMP）模式和 Mesh 模式。

3．WiMAX 网络带宽请求原理

1）PMP 模式带宽请求原理

在 WiMAX 网络的 PMP 模式中，基站控制了上行链路的带宽分配，各个用户站只能通过时间帧的上行子帧向基站发送传输请求。

当应用程序通过用户站访问网络资源时，用户站首先根据该应用程序的服务类型向基站发起连接请求。基站根据相应的接入控制算法决定是否允许该服务接入网络，并把相应的请求结果发送回用户站。只有当该服务被接受时，用户站才能向基站提出带宽请求。在 WiMAX 网络中，时间帧被分为多个小的时间隙（time slot），基站在收到用户站的带宽请求后，根据特定的带宽分配算法为各个用户站分配带宽资源，并设置时间帧的 UL_MAP 部分来通知带宽分配的结果，即各个用户站的可用带宽范围。用户站接收到来自基站的时间帧后，它将分析时间帧的 UL_MAP 部分来得到下一个时间帧的帧结构，从而得到数据传输部分的带宽分配信息。用户站只能在其允许的时间间隙内传输数据。

当基站的可用带宽资源充足时，基站将采用轮询的方式遍历各个用户站，并根据用户站的带宽需求向各个用户站提供带宽资源。当基站的可用带宽资源处于缺乏状态时，用户站通过竞争的方式获取网络资源。用户站在使用竞争方式获取带宽资源时，不同的用户站在请求传输机会（Transmission Opportunities，TO）时会发生请求碰撞。当前，IEEE 802.16 标准使用截断二进制指数后退的方式来协调各个用户站在带宽请求阶段和初始连接阶段产生的冲突。

2）Mesh 模式带宽请求原理

在 WiMAX 网络的 Mesh 模式中，用户站通过直连或者中继的方式与其他用户站相连，每个用户站与基站一样既是数据接收端又是数据中转发送端。当前，Mesh 模式在 MAC 层中存在两种时隙调度方式：集中式调度（Mesh Centralized Scheduling，Mesh-CS）和分布式调度（Mesh Distributed Scheduling，Mesh-DS），各用户站为其频谱覆盖范围内的网络设备提供数据传输服务。

在 Mesh-CS 调度方式中，Mesh 基站根据各个用户站的带宽请求为各个用户站分配带宽资源；与 WiMAX 网络 PMP 模式不同的是，Mesh-CS 模式中的基站并不参与其管理用户站的数据传输，仅进行无线网络的带宽分配。

在 Mesh-DS 调度方式中，各个用户站通过竞争的方式使用无线网络带宽资源。用户站只有与其邻居节点进行协商，在获得可用带宽时隙的前提下才能进行数据传输。

4．WiMAX 应用场景

WiMAX 作为城域网接入手段，采用了多种技术满足建筑物阻挡情况下的非视距（NLOS）和阻挡视距（OLOS）的传播需求，因此其可以实现非视距传输（这种情形下的传输距离会缩短）。802.16d 主要适用于无线传输和中小型企业接入，802.16e 主要适用于家庭接入和个人终端，支持数据、语音和视频等业务，可与 2G、3G、WLL、WLAN、NGN 等网络混合组网。

固定接入：固定接入业务是 WiMAX 运营网络中最基本的业务模型，类似于固定 DSL 或电缆宽带业务。在这个场景下，不支持便携式连接或切换。SS 可以选择或者将连接改变到最佳的信号的基站。在这个场景下，在 IP 连接建立之前，必须进行鉴权或授权。终端一般为小盒子，一般有室外型的 ODU 和天线，市场容量一般。

游牧式：游牧式业务是固定接入方式发展的下一个阶段，终端可以从不同的接入点，接入一个运营商的 WiMAX 网络，不支持不同基站之间的切换。此种应用可以和固定接入同时提供。

便携式：便携式业务是游牧式发展的下一个阶段，在步行速度下具有有限的切换能力。当终端静止不动时，便携式业务的应用模型与固定式业务和游牧式业务相同。此应用场景主要面向家庭接入和商务人士用户市场，终端一般为 PCMCIA 卡，放置在便携机里；市场容量较大。

全移动：支持车速移动下无中断的应用，面向个人用户市场，可漫游切换，终端一般为 PDA；市场容量很大。

1.6.4.8　Ad hoc 网络

Ad hoc 网络是一种特殊的无线移动通信网络，它是由一组带有无线收发装置的移动终端组成的一个多跳的临时性自治系统。Ad hoc 网络的前身是分组无线网（packet radio network，PRNET）。对分组无线网的研究源于军事通信的需要，并已经持续了近 30 年。早在 1972 年，美国国防部高级研究规划署（DARPA）就启动了分组无线网项目，研究分组无线网在战场环境下数据通信中的应用。PRNET 项目完成之后，DARPA 又在 1983 年启动了高残存性自适应网络项目，研究如何将 PRNET 的成功加以扩展，以支持更大规模的网络。此外，还要开发能够适应战场快速变化环境需要的自适应网络协议。1994 年，DARPA 又启动了全球移动信息系统项目。对能够满足军事应用需要的、可快速展开、高抗毁性的移动信息系统进行全面深入地研究。成立于 1991 年 5 月的 IEEE 802.11 标准委员会采用了“Ad Hoc 网络”一词来描述这种特殊的自组织、对等式、多跳无线移动通信网络，Ad hoc 网络就此诞生。IETF 则将 Ad hoc 网络称为移动 Ad hoc 网络（Mobile Ad Hoc NETwork，MANET）。

1．Ad hoc 基本概念

“Ad Hoc”一词来源于拉丁语，其意思是“特别的，临时的”。Ad hoc 网络是由一组

带有无线收发装置的移动终端组成的一个多跳的临时性自治系统。网络中的移动终端具有路由和报文转发功能，可以通过无线连接构成任意的网络拓扑。这种网络可以独立工作，也可以接入 Internet 或蜂窝无线网络。在后一种情况下，移动 Ad hoc 网络通常是以末端子网的形式接入现有网络。考虑到带宽和功率的限制，移动 Ad hoc 网络一般不适于作为中间承载网络。它只允许产生于或目的地是网络内部节点的信息进出，而不让其他信息穿越本网络，从而大大减少了与现有 Internet 互操作的路由开销。

Ad hoc 网络的节点同时具有移动终端和路由器的功能，因此节点通常包括主机、路由器和电台三部分。其中主机部分完成移动终端的功能，包括人机接口、数据处理等；路由器部分主要负责维护网络的拓扑结构和路由信息，完成报文的转发功能；电台部分提供无线传输功能。从物理结构上分，节点可以分为以下几类：单主机单电台、单主机多电台、多主机多电台、多主机单电台。手持机一般采用单主机单电台，复杂的车载台可能包括通信车内的多个主机，它可以采用多主机单/多电台结构，以实现多个主机共享一个或多个电台。多电台使节点具有更大的灵活性和自适应能力。

由于节点的能力通常相同并可以移动，使得 Ad hoc 网络不适用采用集中式控制结构，因此，Ad hoc 网络一般有两种结构：平面结构和分级结构。平面结构中所有节点的地位平等，所以又可以称为对等式结构。在分级结构中，网络被划分为簇（cluster）。每个簇由一个簇头（cluster header）和多个簇成员（cluster member）组成。这些簇头又组成了更高一级的网络。在分级结构中，簇头节点负责簇间数据的转发，它可以预先指定，也可以由节点使用算法选举产生。根据不同的硬件配置，分级结构的网络又可以被分为单频率分级和多频率分级两种，这里的频率应理解为信道。

根据 Ad hoc 网络的特征，参照 OSI 的七层协议模型和 TCP/IP 的体系结构，可以将 Ad hoc 网络的协议划分为 5 层，分别是物理层、链路层、网络层、传输层和应用层。每层独立地设计和操作，各层间的接口是静态的并与网络的约束和应用的需求无关。为了满足 Ad hoc 网络的特殊要求，需要一种能够在协议体系的多个层支持自适应和优化性能的跨层协议体系结构，并根据所支持的应用来设计系统，即采用基于应用和网络特征的跨层体系结构。

2．Ad hoc 网络特点

与传统通信网络相比，Ad hoc 网络具有以下显著特点。

（1）独立组网：Ad hoc 网络具有独立组网能力，即网络的布设无须依赖于任何预先架设的网络设施。节点开机后就可以快速、自动地组成一个独立的网络。

（2）无中心：Ad hoc 网络采用无中心结构，所有节点的地位平等，组成一个对等式网络，其中的节点可以随时加入和离开网络，任意节点的故障不会影响整个网络的运行。与有中心网络相比，Ad hoc 网络具有很强的抗毁性。

（3）自组织：Ad hoc 网络没有严格的控制中心，所有节点通过分层的网络协议和分布式算法协调各自的行为。无中心和自组织特点使得 Ad hoc 网络可以实现快速自动

组网。

（4）多跳路由：由于发射功率的限制，节点的覆盖范围是有限的。当要与其覆盖范围之外的节点进行通信时，需要中间节点的转发，即要经过多跳。与普通网络中的多跳不同，Ad hoc 网络中的多跳路由是由普通节点共同协作完成的，而不是由专门的路由设备完成的。

（5）动态拓扑：Ad hoc 网络中，移动终端能够以任意可能的速度和移动模式移动，并且可以随时关闭电台，加上无线发送装置的天线类型多种多样、发送功率的变化、无线信道间的随时干扰、地形和天气等综合因素的影响，移动终端间通过无线信道形成的网络拓扑随时可能发生变化，而且变化的方式和速度都难以预测。在网络拓扑图中，这些变化主要体现为节点和链路的数量及分布的变化。

（6）特殊的无线信道特征：Ad hoc 网络采用无线传输技术，由于无线信道本身的特性，它所能提供的网络带宽相对于有线信道要低得多，并且无线信道的质量较差。考虑到竞争共享无线信道的冲突、信号衰减、噪音和信道之间干扰等因素，移动终端获得的实际带宽远远小于理论上的最大带宽，并且会随时间动态地发生变化。在 Ad hoc 网络中，节点的发送功率受限，一个节点的发送，只有其一跳相邻节点可以听到，而此范围之外的其他节点觉察不到。这一特征一方面提高了信道的空间复用度，另一方面使得报文的冲突与节点所处的地理位置相关。此外，地形和发射功率等因素使得 Ad hoc 网络中可能存在单向无线信道。例如，车载终端的发送功率大于手持终端，手持终端可以收到来自车载终端的信号，而车载终端无法收到来自手持终端的信号，即存在从车载终端到手持终端的单向信道。

（7）移动终端的局限性：移动终端具有便携方便、轻便灵巧等优点，但也存在其固有的缺陷，如能源受潮，内存较小、CPU 处理能力较低和成本较高等，从而给设计开发和应用推广带来一定难度，同时显示屏等外设的功能和尺寸受限，不利于开展功能较复杂的业务。考虑到成本和易于携带，移动节点不能配备太多数量的发送接收器，并且节点一般依靠电池供电。因此如何高效地使用节点的电能和延长节点的工作时间是一个十分突出的问题。

（8）安全性差：Ad hoc 网络是一种特殊的无线移动网络，由于采用无线信道、有限电源、分布式控制等技术，它更加容易受到被动窃听、主动入侵、拒绝服务、剥夺“睡眠”等网络攻击。此外，Ad hoc 网络由节点自身充当路由器，不存在命名服务器和目录服务器等网络设施，也不存在网络边界的概念。这就使得 Ad hoc 网络中的安全问题非常复杂，传统网络中的许多安全策略和机制将不再适用。因此，信道加密、抗干扰、用户认证、密钥管理、访问控制和其他安全措施都需要特别考虑。

3. 应用背景

Ad hoc 网络的许多优良特性为它在民用和军事通信领域占据一席之地提供了有利的保证。首先，网络的自组织特性提供了廉价而且快速部署网络的可能。其次，多跳和

中间节点的转发特性可以在不降低网络覆盖范围的条件下减少每个终端的发射功率，从而降低了天线和相关发射/接收部件的设计难度和成本，为移动终端的小型化、低功率提供了可能。从共享无线信道的角度看，Ad hoc 网络降低了信号冲突的概率，提高了信道利用率。从用户的角度看，低功率的无线电波产生的电磁辐射较小，对人身体的影响较小。低功率的无线电波也减少了被截获和监听的概率。

Ad hoc 网络的应用可以归纳为以下几类。

（1）军事应用：军事应用是 Ad hoc 网络技术的主要应用领域。因其特有的无须架设网络设施、可快速展开、抗毁性强等特点，移动 Ad hoc 技术已成为数字化战场通信的首选技术。在近年来得到迅速发展的美军战术互联网中，Ad hoc 网络技术是它的核心技术。为了满足信息战和数字化战场的需要。美军研制了大量的无线自组织网络设备，用于单兵、车载、指挥所等不同的场合，并大量装备部队。在伊拉克战争中，移动 Ad hoc 网络得到了有效的应用。

（2）传感器网络：传感器网络是 Ad hoc 网络技术应用的另一大领域。对于很多应用场合来说，传感器网络只能使用无线通信技术。而考虑到体积和节能等因素，传感器的发射功率不可能很大，使用 Ad hoc 网络实现多跳通信是非常实用的解决方法。分散的传感器通过 Ad hoc 网络技术组成一个网络，可以实现传感器之间和与控制中心之间的通信。这种网络在军事应用、道路交通、工业制造、生物医药以及各种安全场合都具有非常广阔的应用前景。

（3）紧急场合：在发生了地震、水灾、火灾或遭受其他灾难打击后，固定的通信网络设施可能全部损毁或无法正常工作。这时就需要 Ad hoc 网络这种不依赖任何固定网络设施又能快速布设的自组织网络技术，在这些恶劣和特殊的环境下提供通信支持，这对抢险和救灾工作具有非凡的意义。

（4）偏远野外：当处于偏远或野外地区时，无法依赖固定或预设的网络设施进行通信。Ad hoc 网络技术具有单独组网能力和自组织特点，是这些场合通信的最佳选择。其应用包括野外科考队、边远矿山作业、边远地区执行任务分队的通信等。

（5）临时场合：Ad hoc 网络的快速、简单组网能力使得它可以用于临时场合的通信。比如会议、庆典、展览等场合，可以免去布线和部署网络设备的工作。在室外临时环境中，工作团体的所有成员可以通过 Ad hoc 方式组成一个临时网络来协同完成一项大的任务，或协同完成某个计算任务。在室内办公环境中，办公人员携带的包含 Ad hoc 收发器的 PDA，可以通过无线方式自动从台式机上下载电子邮件，更新工作日程表等。

（6）动态场合：对于像执行运输任务的汽车队这样的动态场合，Ad hoc 网络技术也可以提供很好的通信支持。美国加州大学伯克利分校和哈佛大学正在研究如何将 Ad hoc 网络技术应用于高速公路自动驾驶汽车间的通信，并取得了初步的研究成果。

（7）个人通信：个人局域网是 Ad hoc 网络技术的又一大应用领域。用户实现 PDA、手机、掌上电脑等个人电子通信设备之间的通信，并可以构建虚拟教室和讨论组等崭新

的移动对等应用。考虑到辐射问题，个人局域网通信设备的无线发射功率应尽可能小，这样 Ad hoc 网络的多跳通信能力将再次展现它的过人之处。蓝牙的超网（scatternet）技术就是一个典型的例子。

（8）商业应用：使用 Ad hoc 网络技术可以组建家庭无线网络、移动医疗监护系统，开展移动和可携带计算等。比如未来装备 Ad hoc 收发设备的机场预约和登机系统可以自动地与乘客携带的个人无线 Ad hoc 设备通信，完成目前的换登机牌等手续，节省排队等候时间。

（9）其他场合：由于 Ad hoc 网络的特殊特点，它的应用领域还很多，这需要进一步去发掘。不如它可以用于扩展现有蜂窝移动通信系统的覆盖范围，实现地铁和隧道等场合的无线覆盖；构建未来的无线城域网和自组织广域网等。

1.6.5　接入网

接入网（Access Network，AN）除了包含用户线传输系统、复用设备外，还包括数字交叉连接设备和用户/网络接口设备。接入网为本地交换机（LE）与用户端设备（TE）之间的实施系统，其目的是综合考虑本地交换局、用户环路和终端设备，通过有限的标准化接口将各种用户所需求的业务接入节点。

接入网的引入给通信网带来新的变革，使整个通信网络结构发生了根本的变化。然而，接入网一直是通信网中耗资最大、技术变化最慢、成本最敏感和运行环境最恶劣的领域。

当核心网和用户驻地网频繁地更换和应用各种现代新技术时，接入网领域基本维持着原始的模拟技术和窄带接入技术为主的局面。显然，接入网技术已成为制约通信发展的瓶颈。为了给用户提供端到端的宽带连接，保证宽带业务的开展，网络的宽带化、数字化是接入网的前提和基础，同时也是网络技术中的一大热点。接入网的技术实现手段有多种，当前各种宽带接入技术都在发展和应用中。

1.6.5.1　拨号接入

PSTN 用户通过公共交换电话网（PSTN）拨号进入 Internet，即 PSTN 用户通过拨号在用户 PC 与 Internet 服务提供者（ISP）之间建立一条物理电路。由于 PSTN 用户线为模拟用户线，所以在用户端需加装频带调制解调器（modem）进行数据信号与音频话带信号之间的转换。

在电话网与 ISP 运营商网络（ISP/LAN）之间装有接入服务器（AS）。AS 对电话网提供 Modem Pool、E1 话路中继及中国一号、NO.7 信令接口。AS 对 ISP/LAN 提供以太网接口。在 ISP/LAN 中装有 WWW、DNS、AAA、E-mail、计费等服务器并通过路由器或路由交换机进入 Internet。

Modem 是一个数字信号与模拟信号之间的转换设备。只需利用现有的电话线路和一

个 Modem，用户即可连入到 Internet。这种接入方式简单易行、价格低廉，早期一度成为单机用户接入 Internet 的主要方式。但因为要进行数字信号与模拟信号之间的转换，所以该方式网络连接速度低，而且性能较差。随着时代的发展，文本、图形、图像、音频、视频、动画等大数据量信息的传输在不断地增多，这样，价格低廉但传输速度较慢的 Modem 接入技术显然是无法胜任的。因而，Modem 拨号接入技术面临着逐渐被淘汰的局面。

1.6.5.2 ISDN 接入

窄带 ISDN（N-ISDN）用户利用 2B+D 数字用户线拨号上网。其中的 B 通道为业务通道，其速率为 64kbps；D 通道为信令通道，其速率为 16Kbps。通常可利用其中一个 B 通道通话，另一个 B 通道上网，故 N-ISDN 俗称“一线通”。在局端“一线通”用户数据流经由 ISP/LAN 和路由器进入 Internet。N-ISDN 的 D 通道永远在线用于传送用户信令和低速分组数据。

N-ISDN 将电话语音和计算机多媒体数据集成到一条高速的数字传输网络线路中，仅通过一路“线路”就可以为客户同时提供语音服务和数据服务。“一线通”虽基于现有的公众电话网，通信线路就是普通的电话线，使用方法与使用普通电话没有区别。但与普通的模拟电话不同的是，“一线通”在线路上传输的是数字信号，而非被处理之后的模拟信号，使用户完全步入“数字化通信”时代。它具有以下特点。

（1）一线多能：利用一对用户线可实现电话、传真、可视图文、数据通信等多种业务的通信。

（2）连接速度快，使用灵活。

（3）成本低、连接质量好。由于使用了数字传输技术，信号的误码率要比模拟线路低得多，而且断线现象明显减少。

随着 Internet 和企业计算机联网的日益普及，“一线通”在数据通信领域的优势还是受到了人们关注，“一线通”具有一定数量的用户，但逐步会被 ADSL 接入所取代。

1.6.5.3 xDSL 接入

数字用户线路（Digital Subscriber Lines，DSL）由于采用了先进的数据调制技术，通过普通的电话线就可以达到非常高的吞吐量。xDSL 是对所有不同 DSL 的总称。DSL 的类型可以分为两大类，即非对称 DSL 和对称 DSL。目前共有 7 种 DSL。比较有名的 DSL 类型包括非对称 DSL（ADSL）、高比特率 DSL（HDSL）、单线 DSL（SDSL）以及超高比特率 DSL（VDSL）。其中 ADSL 和 VDSL 使用最广。

1．ADSL 接入

非对称数字用户环路（ADSL）是一种上、下行传输速率不等的高速数字用户环路，且在同一对用户线上还可同时传送传统的模拟话音信号。在用户端 PC 或机顶盒通过

ATU-R（远端 ASDL Modem）和模拟话音分离器接入用户铜线。在局端用户线通过分离器接入 ATU-C（局端 ADSL Modem），并经由数字用户线路接入复用器（Digital Subscriber Line Access Multiplexed，DSLAM）进行复接。复接后的高速数据流经由 ISP/LAN 和路由器进 Internet。

在 ADSL 系统中，ADSL 收发信机从一对用户线中辟出三个通道：普通电话业务（POTS）信道、中速双工数据信道、高速下行数据信道。普通电话业务占据 4kHz 以下的基带，并通过无源低通滤波器与数字信号分离以保证在 ADSL 系统出现故障情况仍能保证通话业务。上行信道数据速率为 16Kbps～1Mbps；下行信道包括一个中速双向信道的下行部分（速率同上行信道）和一个高速（1.5Mbps～9Mbps）单工下行通道。这三个通道可以同时工作。在实际应用中频段划分视设备而异。各信道数据速率与占用线路频宽及调制效率（码速率/调制符号速率）有关。

ADSL 系统是针对住宅用户设计的，目前 ADSL 大多用于高速接入 Internet 业务。并能享用 ISP 运营商所提供的诸如点播电视、远程教学、远程医疗、居家购物、可视电话、多方可视游戏等多媒体业务。

2．VDSL 接入

由于 ADSL 技术在提供图像传输时下行宽带十分有限，而且成本偏高。在提高系统下行带宽过程中系统逐步演变为甚高比特数字用户环路（VDSL）。

VDSL 系统用于接入网中的最后一段入户连接。其传输距离只有 300m（52Mbps 时）～1km（13Mbps 时）。其传输速率为：下行达 13Mbps～52Mbps；上行为 1.5Mbps～2Mbps。

由于 VDSL 系统传输距离缩短，码间干扰大大减小，对数字信号处理要求亦大为简化，收发信机成本有望比 ADSL 降低一半。

VDSL 系统因传输距离短，故一般作为光纤到路边（FTTC）和光纤到大楼（FTTB）的宽带延伸。从目前看来 VDSL 和 ATM 无源接入网（APON）混合使用是一种比较理想的宽带接入方案。

1.6.5.4 Cable Modem 接入

电缆调制解调器（cable modem）是适用于电缆传输体系的调制解调器。它基于有线电视网络，利用了有线电视电缆可以同时传输多个频道的工作机制，使用电缆带宽的一部分来传送数据。Cable Modem 是将数据进行调制后在电缆的一个频率范围内传输，接收时进行解调，传输机理与普通 Modem 相同。不同之处在于它是通过有线电视网络的某个传输频带进行调制解调的。而普通 Modem 的传输介质在用户与交换机之间是独立的，即用户独享通信介质。Cable Modem 属于共享介质系统，其他空闲频段仍然可用于有线电视信号的传输。

Cable Modem 类似于电话线上使用的音频 Modem，其主要作用是完成数字信号的远距离传送。Cable Modem 下行载波带宽 6MHz，数据速率在采用 64QAM 调制方式时为

31.2Mbps；采用 256QAM 调制方式时为 41.6Mbps。上行采用 QPSK 或 16QAM 调制方式在 200KHz~3.2MHz 带宽范围内，数据速率可达 320Kbps~10Mbps，多个用户 Cable Modem 上行信号可在同一载波上分时隙发送。

我国现在开通的 Cable Modem 接入业务基本上是基于双向的混合型光纤同轴电缆（HFC）的。Cable Modem 的技术具有以下特点：

（1）连接速度快。在目前应用的所有接入方式中，Cable Modem 是最快的一种。

（2）成本低廉。Cable Modem 利用已有的有线电视网络。

（3）提供了非对称的专线连接。Cable Modem 是一直在线的，用户无须拨号，也不用担心遇着忙音，只要一打开计算机就会自动建立与 Internet 的高速连接。

（4）不受连接距离的限制。用户所在地和有线电视中心局之间的同轴电缆能够按照用户的需要延伸，不受连接距离的限制。

Cable Modem 技术同样也存在着一些不足：Cable Modem 用户共享单一电缆的方式与局域网中多台计算机共享信道相似，由于许多用户通过一个节点接入 Internet，如果所在区域的上网用户较多时，传输速率将明显下降。另外，有线电视是一种广播服务，所以同一信号将发送给所有的用户，用户端的 Cable Modem 会对信号进行识别。如果是发给自己的便将其分享出来，并接收。这种工作方式会产生一些安全问题：其他用户可能会共享电缆访问正在传输的数据。

1.6.5.5 局域网接入

当前 90%的局域网采用以太网（Ethernet）技术组网。以太网的传输速率高、组网设备价格低廉，其传输链路可采用光纤、同轴电缆、铜缆双绞线等物理媒体。随着以太网技术的迅速发展，该技术进入 IP 城域网和接入网领域。

目前新建住宅小区和商务楼流行局域网（LAN）方式接入。小区接入节点（ZAN）提供住宅小区接入，采用千兆以太网交换机；楼宇接入点（BAN）提供居民楼宇接入，采用百兆以太网交换机，实现住宅小区的千兆光纤到小区、百兆光纤或 5 类线到住宅楼、十兆 5 类线到用户的宽带用户接入方案；或商务楼的千兆到大楼、百兆到楼层、十兆到用户的用户接入方案。小区或大楼的千兆光纤经由 IP 城域网汇聚层的路由交换机进入城域核心网。

城域网的汇聚层将电话、数据以及各种宽带多媒体接入业务，汇聚为 IP（ATM）数据流进入城域骨干网。汇聚层可提供诸如点播电视、有线电视、信息广播等一些业务。该层还有一个重要作用是对用户进行鉴权、认证、计费和管理。用于汇聚层的典型设备包括各类路由器、路由交换机、各类网关、宽带综合接入服务器、WWW、DNS（域名）、AAA（鉴权、认证、计费）等服务器以及各类信息源。

1.6.5.6　无线接入

1．无线接入技术

无线接入技术是无线通信的关键问题，是指通过无线介质将用户终端与网络节点连接起来，以实现用户与网络间的信息传递。无线信道传输的信号应遵循一定的协议，这些协议即构成无线接入技术的主要内容。无线接入技术与有线接入技术的一个重要区别在于可以向用户提供移动接入业务。

无线接入大致可分为三种：

1）低速无线本地环

无线本地技术源于 20 世纪 40 年代中期出现的蜂窝电话和随后产生的无绳电话等移动通信技术。最常用的为蜂窝通信技术，即利用模拟蜂窝移动通信技术，如总访问通信系统、高级移动电话服务系统等。这类技术的速率较低，像全球通仅能够提供 13Kbps 语音服务和 9.6Kbps 的数据服务。

2）宽带无线接入

随着无线接入市场的不断扩大，许多无线设备制造商开始提供基于无线电波的宽带接入系统， 如多路多点分配业务和本地多点分配业务。这些系统采用数字技术，并支持多用户和多种服务，数据通信速率一般在 128Kbps～155Kbps。

3）卫星接入

卫星接入就是利用卫星通信系统提供的接入服务。它由人造卫星和地面站组成，用卫星作为中转站转发传入的无线电信号。其中，能够为用户提供电话、电视和数据接入服务的卫星接入业务，在我国已有了较广泛的应用。

2．宽带无线接入

宽带无线接入技术虽然没有像 ADSL 等有线宽带技术那样成为主流的接入手段，但是由于它自身的优点，在整个宽带市场中也占据了一席之地，网络规模逐年扩张。

与传统仅提供窄带话音业务的无线接入技术不同，宽带无线接入技术（BWA）面向的主要应用是 IP 数据接入和话音接入。BWA 的出现源于 Internet 的发展和用户对宽带数据需求的不断增长。各个国家从 1999 年开始纷纷为 BWA 分配频率，其中主要包括 2.5GHz、3.5GHz、5GHz、24GHz、26GHz 等频段。北美国家主要分配了 2.5GHz，欧洲的国家则主要分配了 3.5GHz 频率资源。20GHz 以上的宽带无线接入技术统称为本地多点分配技术（LMDS）。我国为 BWA 分配的频率资源包括 3.5GHz，5.8GHz，26GHzLMDS，其中 5.8GHz 为扩频通信系统、宽带无线接入系统、高速无线局域网、蓝牙系统等共享的频段，其余两个频带则是宽带无线接入专有频带。

当前宽带无线接入有以下几大技术：LMDS（Local Multipoint Distribute System，本地多点分配系统）、MMDS（Multipoint Multichannel Distribution System，多点多信道分配系统）、无线局域网、蓝牙及其他（如红外等）。

1）LMDS（高频宽带、24/26GHz～38GHz）

LMDS 频谱资源比较多，可以传输较高的速率，但是由于工作于毫米波，受气候影响大，抗雨衰性能差，降低了在经济发达的东南沿海地区的可用度。目前通常所说的 LMDS 为第二代数字系统，主要使用无线 ATM 传送协议，具有标准化的网络侧接口和网管协议。LMDS 具有更高带宽和双向数据传输的特点，可以提供多种宽带交互式数据业务及话音和图像业务，因此人们逐渐将眼光投入带宽达到 1GHz，几乎可以提供任何种类的业务。我国已完成频率规划，频段为 24.507GHz～25.515GHz 和 25.757GHz～26.765GHz。

2）MMDS（中频中宽带、2GHz～5GHz）

该频段传输性能好，覆盖范围广，技术成熟，具有良好的抗雨衰性能，扩容性强，组网灵活且成本具有竞争力，是较为理想的无线接入手段。由于该频段资源比较紧张，能分给 MMDS 的频段窄、信道数少，需用新技术来提高频谱利用率。中国（3.4GHz～3.43GHz 和 3.5GHz～3.53GHz）已经分配试用。因为频段相对紧张，所以格外激发了高效利用频率的新技术的大量涌现。

3）无线局域网 WLAN

无线局域网的主要技术有 IEEE 802.11b、IEEE 802.11a、IEEE 802.11g、HiperLAN 等。当前最具代表性的当数 IEEE 802.11b。1999 年 9 月通过的 IEEE 802.11b 工作在 2.4GHz～2.483GHz 频段。与有线局域网的不同主要体现在便携性上。WLAN 技术发展较为迅速，由于 IEEE 802.11 标准成功解决了空中接口兼容性问题，促进了无线局域网终端和接入点（AP）的互通，因此 WLAN 设备成本下降很快，应用也非常广泛。

虽然 WLAN 的公众热点数在增多，但是对于 WLAN 技术，由于每个 AP 的覆盖范围有限，因此整个热点内 AP 的互联也需要有线网络设施的支撑，对网络整体投资有一定的要求。

4）蓝牙

蓝牙也是一种使用 2.4GHz～2.483GHz 的无线频带（ISM 频带）的通用无线接口技术，提供不同设备间的双向短程通信。蓝牙的目标是最高数据传输速率 1Mbps（有效传输速率为 721Kbps）、最大传输距离为 10cm～10m（增加发射功率可达 100m）。蓝牙的优势是设备成本低、体积小。而且，搭配“蓝牙”构造一个整体网络的成本要比铺设线缆低。相对 802.11x 系列和 HiperLAN 家族，蓝牙的作用不是为了竞争而是相互补充。

宽带无线接入技术经过近几年的发展，已经形成了一定的产业规模。随着新的技术涌现，宽带无线接入的传输能力在不断增强，接口更加开放，技术的发展正经历从固定到移动的发展过程。

1.6.5.7 光网络接入

1．光纤接入技术

光纤接入网是指局端与用户之间完全以光纤作为传输媒体。接入网光纤化有很多方

案，有光纤到路边（FTTC）、光纤到小区（FTTZ）、光纤到办公楼（FTTB）、光纤到楼面（FTTF）、光纤到家庭（FTTH）。采用光纤接入网是光纤通信发展的必然趋势，尽管目前各国发展光纤接入网的步伐各不相同，但光纤到家庭是公认的接入网发展目标。现阶段大规模实现FTTH还不经济，主要是实现FTTB/FTTC，目前可采用的传送技术手段以有源光纤接入（如PDH、ATM、SDH、GE/FE等）为主，但当无源光纤接入开始得到应用时，其将成为FTTH的一种最经济有效的技术手段。

毫无疑问，光纤是接入网的理想传输媒介。光纤接入网具有以下优点：

（1）光纤接入网能满足用户对各种业务的需求。人们对通信业务的要求越来越高，如果要提供高清晰度或交互式视频等业务，用铜线双绞线是难以实现的。

（2）光纤可以克服铜线电缆无法克服的一些限制因素，且损耗低、频带宽，解除了铜线电缆网径小的限制，此外，光纤不受电磁干扰，保证了信号传输质量。

（3）光纤接入网的性能不断提高，价格不断下降。

（4）光纤接入网提供数字业务，有完善的监控和管理系统，能适应将来宽带综合业务的需要，打破有限带宽的传输瓶颈，使信息高速公路畅通无阻。

现在，影响光纤接入网发展的主要原因不是技术，而是成本。直至目前，光纤接入网的成本仍然较高。

2. 光纤接入网的分类

光纤接入网可以粗分为有源和无源两类。有源接入依然是目前光纤接入的主要手段，典型的设备主要是基于 SDH 的多业务传送平台（Multi-Service Transport Platform，MSTP）、基于以太网或 ATM 的多业务接入平台等。然而，这种技术作为有源设备仍然无法完全摆脱电磁干扰和雷电影响，以及有源设备固有的维护问题。尽管它在中近期会有所发展，但不是接入网的长远解决方案。无源光网络（PON）是一种很有吸引力的纯介质网络，其主要特点是避免了有源设备的电磁干扰和雷电影响，减少了线路和外部设备的故障率，提高了系统可靠性，同时节省了维护成本，PON由于简洁、廉价、可靠的网络拓扑结构，被普遍认为是宽带接入网的最终解决方案。

3. 无源光网络

PON技术是最新发展的点到多点的光纤接入技术。无源光网络由光线路终端（OLT）、光网络单元（ONU）和光分配网络（ODN）组成。一般其下行采用TDM广播方式、上行采用TDMA（时分多址接入）方式，而且可以灵活地组成树型、星型、总线型等拓扑结构（典型结构为树型）。PON的本质特征就是ODN全部由无源光器件组成，不包含任何有源电子器件，这样避免了外部设备的电磁干扰和雷电影响，减少了线路和外部设备的故障率，提高了系统可靠性，同时节省了维护成本。与有源光接入技术相比，PON由于消除了局端与用户端之间的有源设备，从而使得维护简单、可靠性高、成本低，而且能节约光纤资源。

目前PON技术主要有APON（基于ATM的PON）、EPON（基于以太网的PON）

和 GPON（Gigabit PON）等几种，其主要差异在于采用了不同的二层技术。

1）APON

APON 是 20 世纪 90 年代中期被 ITU 和全业务接入网论坛（FSAN）标准化的 PON 技术，在 2001 年底 FSAN 又将 APON 更名为 BPON，APON 的最高速率为 622Mbps，二层采用的是 ATM 封装和传送技术，因此存在带宽不足、技术复杂、价格高、承载 IP 业务效率低等问题，未能取得市场上的成功。

2）EPON

为更好适应 IP 业务，第一英里以太网联盟（EFMA）在 2001 年初提出了在二层用以太网取代 ATM 的 EPON 技术，IEEE 802.3ah 工作小组对其进行了标准化，EPON 可以支持 1.25Gbps 对称速率，将来速率还能升级到 10Gbps。EPON 产品得到了更大程度的商用，由于其将以太网技术与 PON 技术完美结合，因此非常适合 IP 业务的宽带接入技术。对于 Gbps 速率的 EPON 系统也常被称为 GE-PON。

3）GPON

在 EFMA 提出 EPON 概念的同时，FSAN 又提出了 GPON，FSAN 与 ITU 已对其进行了标准化，其技术特色是在二层采用 ITU-T 定义的 GFP（通用成帧规程）对 Ethernet、TDM、ATM 等多种业务进行封装映射，能提供 1.25Gbps、2.5Gbps 下行速率和所有标准的上行速率，并具有强大操作、管理、维护和配置（Operation Administration Maintenance and Provisioning，OAM&P）功能。在高速率和支持多业务方面，GPON 有明显优势，但目前成本要高于 EPON，产品的成熟性也逊于 EPON。

1.6.6 广域网组网

广域网组网可划分为三级网络：第一级为骨干网，第二级为分布网，第三级为接入网。网络规模不大时可直接由骨干网和接入网组成。

在组网时，根据广域网网络的规模和业务的需要对三级网络的功能进行规划。例如某省级银行的广域网设计为：第一级骨干网，支持数据、话音、图像等多元化信息共享，为全行系统提供高速、可靠的通信服务。第二级分布网，用于数据中心与各分支行的数据交换，能提供长途线路复用和主干访问。第三级接入网用于各分支行与各营业网点的数据交换，采用访问路由方式，提供网点线路复用和终端访问。

1.7 网络互连

1.7.1 网络互连概念

网络互连（internetworking）是指利用各种网络互连设备将同一类型的网络或不同类型网络及其产品相互连接起来组成地理覆盖范围更大、功能更强的网络。网络互连也可

以理解为将一个网络分解为若干个子网，它是计算机网络发展到一定阶段的必然产物。

网络互连的目的是使得一个网络上的某一台主机能够与另一个网络上的主机进行通信。为了完成这个目标，提出了许多方法来提供网络互连服务，但是这些服务要满足以下几条要求：

- 提供网络间的链路。至少必须提供物理和链路层的连接。
- 提供不同网络中的进程间的数据的路由选择和传递。
- 提供记账服务，跟踪各个网络和路由器的使用情况，并记录这些状态信息。
- 必须能够适应网络间的许多差异，而不需要变更所连接网络的体系结构。

网络互连为使用者提供了便利，它具有以下优点：

- 扩大资源共享的范围。更多的资源可以被更多的用户共享。
- 提高网络的性能。网络性能会随着网上节点的增加、网络覆盖范围的扩大而降低。
- 降低成本。当同一地区的多台主机希望接入另一地区的某个网络时，采用主机先行联网（局域网或者广域网），再通过网络互连技术达到目的的方法可以大大降低联网成本。
- 提高安全性。将具有相同权限的用户主机组成一个网络，在网络互连设备上严格控制其他用户对该网的访问，从而实现网络的安全机制。
- 提高可靠性。设备的故障可能导致整个网络的瘫痪，而通过子网的划分可以有效地限制设备故障对网络的影响范围。

1.7.2　网络互连方法

网络互连的方法主要包括：局域网-局域网互连（LAN-LAN）、局域网-广域网互连（LAN-WAN）、广域网-广域网互连（WAN-WAN）。

网络互连的层次及所对应的设备关系如图1-64所示。

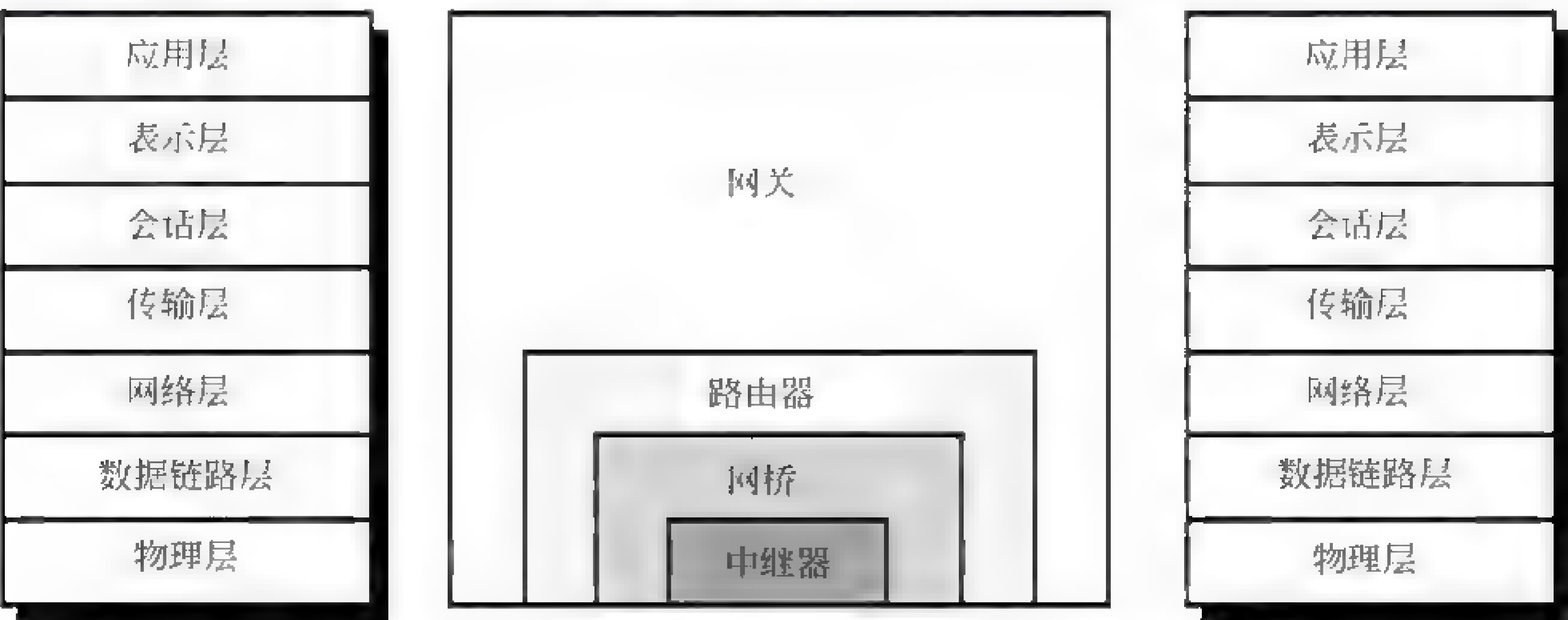


图1-64　网络互连层次及所对应的设备关系

用于网络之间的互连的中继设备称为网络互连设备，按照网络互连设备是对哪一层（可能包括下层）进行协议和功能的转换，可以把它们分成以下 4 类：

- 中继器完成物理层间的互连，主要起到信号再生放大，延长网络距离，也就是把比特流从一个物理段传输到另一个物理网段。
- 网桥完成数据链路层间的连接，可以将两个或多个网段连接起来，网桥在网络互连中起着数据接收、地址过滤与数据转发的作用，用来实现多个网络系统之间的数据交换。主要连接同类局域网络。
- 路由器是进行网络层间的互连，网络层互连主要解决路由选择、拥塞控制、差错处理与分段技术等问题。
- 网关是工作在七层协议参考模型中第三层以上的网间连接设备，它的作用是连接多个高层协议不同的网络，使它们能够相互通信。

1.7.2.1 LAN-LAN

LAN-LAN 网络的互连设备是中继器、集线器和网桥，也可以用路由器。

1. 中继器及其工作原理

中继器又叫转发器，是 LAN 环境下用来延长网络距离的互连设备中最简单、最廉价的设备，其应用如图 1-65 所示。这种设备是物理层设备，即两个网络在物理层上的连接，要求物理层的协议是相同的。之所以这样说是因为它只是简单地将来自一侧的信号转发到另一侧(当为双口中继器时)或将来自一侧的信号转发到多个口，并不关心 0 和 1 的含义。因为它只具有信号放大再生之类的功能，因此只能连接使用相同媒体访问方法和相同数据传输速率的 LAN。 中继器在执行信号放大功能时不需要任何智能或算法。



图 1-65 用中继器连接两个网段

由于信号在传输中存在损耗，在线路上传输的信号功率会逐渐衰减，衰减到一定程度时将造成信号失真，因此会导致接收错误。中继器就是为解决这一问题而设计的。它完成物理线路的连接，在转发时对衰减的信号进行放大，使信号可以传输更远的距离，且保持与原数据相同。

一般情况下，中继器的两端连接的是相同的媒体，但有的中继器也可以完成不同媒体的转接工作。从理论上讲中继器的使用是无限的，网络也因此可以无限延长。事实上这是不可能的，因为网络标准中都对信号的延迟范围作了具体的规定，中继器只能在此规定范围内进行有效的工作，否则会引起网络故障。

应当注意，使用中继器连接 LAN 的电缆段是有限制的，需遵循一定的网络标准。标准以太网络中就约定了一个以太网上只允许出现 5 个网段，最多使用 4 个中继器，而且其中只有 3 个网段可以挂接计算机终端，简称 5-4-3 规则。即最多只能使用 3 个同轴电缆段，其余必须为链路段。当 5 个段都存在时，粗缆每个链路段不得超过 500m。当通路由 3 个中继器、5 个段组成时，链路段最大长度为 2500m。

使用中继器扩充网络距离是最简单、最廉价的方法，但是使用中继器所扩展的网络所有的连网设备都具有相同的工作带宽，处于一个相同的网段上，常把这种网络称为介质共享网络或共享式局域网。

介质共享网络上的所有设备都处于一个冲突域或碰撞域（Collision Domain）中，它的致命问题是随着接入网络中设备的增加其性能会逐渐下降，并当接入设备的数量达到一定程度后，有些网络会迅速崩溃。所以只有当网络负载很轻和网络时延要求不高的条件下才能使用这种网络。

2. 集线器及其互连原理

1）集线器有关概念

用网络术语来说，集线器（Hub 或 Concentrator）是基于星型拓扑的接线点。集线器的基本功能是信息分发，它把一个端口接收的所有信号向所有端口分发出去。一些集线器在分发之前将弱信号重新生成，一些集线器整理信号的时序以提供所有端口间的同步数据通信。

2）集线器的构成

集线器是中继器的一种形式，也称其为盒装总线，如图 1-66 所示，所以集线器连接的计算机是共享同一网络带宽的。正是因为这个特点，集线器不适合用来构建大型网络。它与中继器的区别在于能够提供多端口服务，也称为多口中继器。集线器也工作在 OSI/RM 中的物理层。

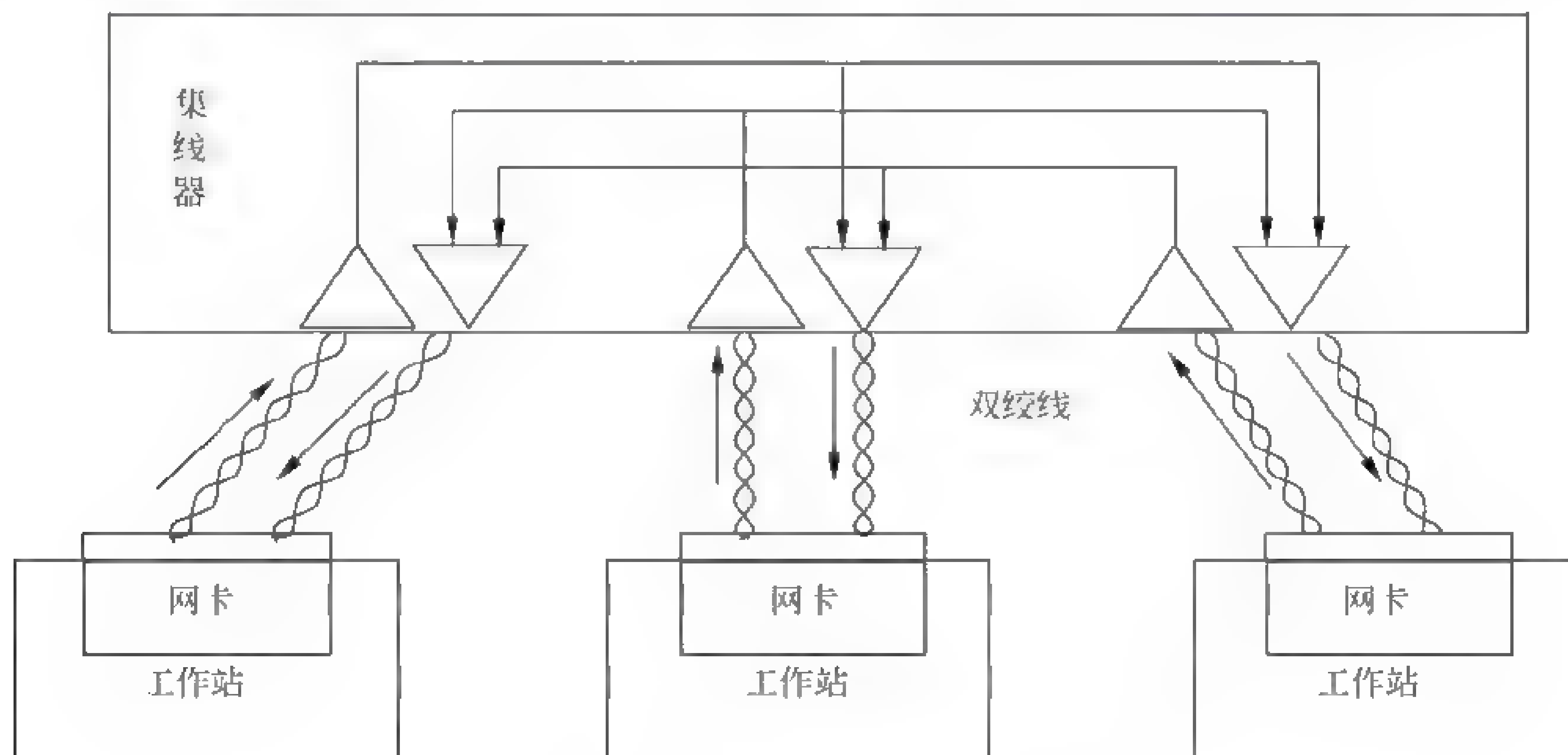


图 1-66　集线器的组成

集线器按端口的传输速率来分，有 10Mbps 和 100Mbps 两种。通常所说的集线器是共享式集线器，其带宽是所有端口共享的。例如一台 16 端口的 100Mbps 的集线器，当全部端口都使用时，每一端口的带宽只有 1/16。由集线器作中心设备的局域网称为共享式局域网。

集线器的全部端口属于一个冲突域，它在端口之间转发数据帧时采用向所有端口广播的方式进行，因此其全部端口又属于同一个广播域（broadcast domain）。单一的冲突域和广播域使网络在通信繁忙时容易产生阻塞和广播风暴。

3）使用集线器扩展局域网

使用集线器扩展 LAN（如图 1-67 所示），使原来属于不同碰撞域的局域网上的计算机能够进行跨碰撞域的通信，扩大了局域网覆盖的地理范围。但同时碰撞域也增大了，总的吞吐量并未提高。当不同碰撞域使用不同数据率时，不能用集线器将它们互连起来。

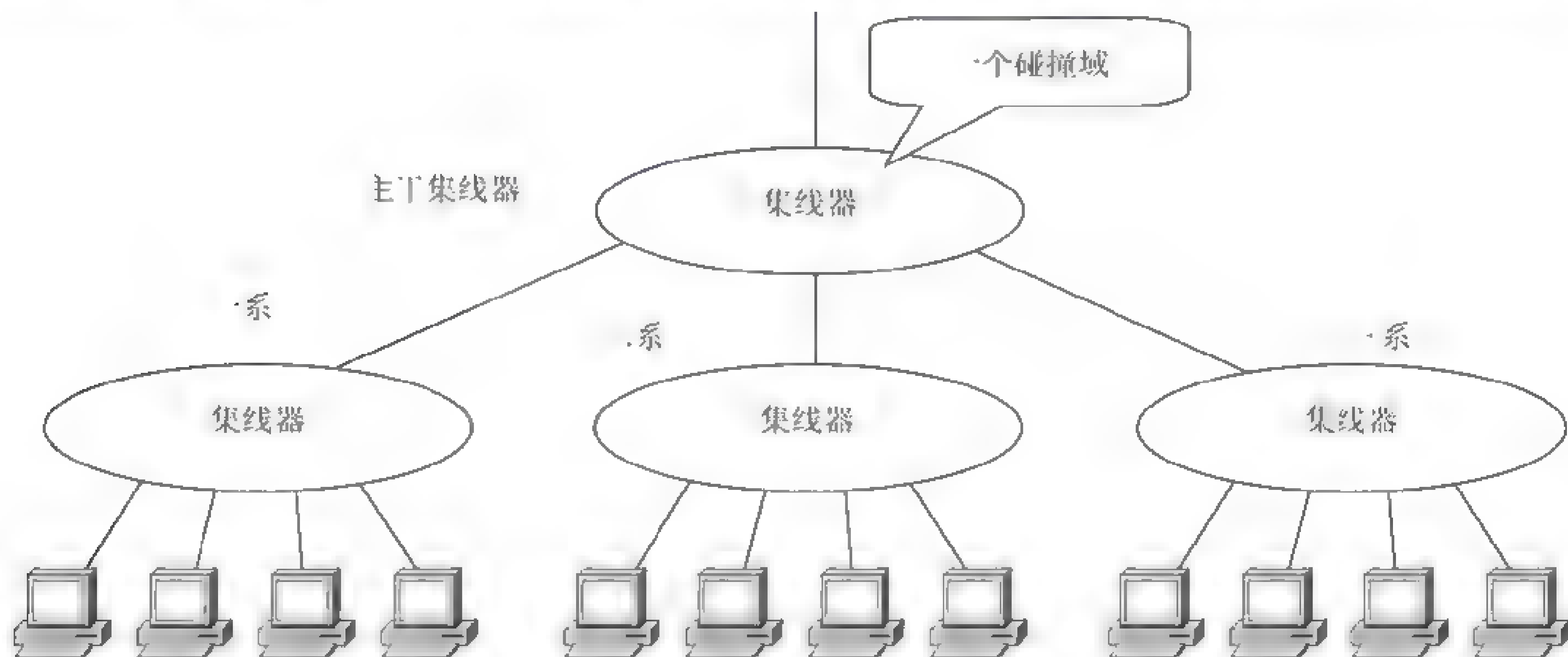


图 1-67　使用集线器扩展局域网

可以使用多台集线器级联或堆叠来增加总的端口数，但不能用此方法来延伸网络距离。目前随着交换机价格的下降，共享式 Hub 正逐渐退出局域网领域。

3. 网桥及其互连原理

1）网桥有关概念

网桥（bridge）也叫桥接器，是连接两个局域网的一种存储/转发设备，它能将一个较大的 LAN 分割为多个网段，或将两个以上的 LAN 互连为一个逻辑 LAN，使 LAN 上的所有用户都可访问服务器。它工作在数据链路层，它根据 MAC 帧的目的地址对收到的帧进行转发。

网桥具有以下几个基本特征：

- 能够连接两个采用不同数据链路层协议、不同传输介质与不同传输速率的网络。
- 以接收、存储、地址过滤与转发的方式，实现互连的网络之间的通信。

- 要求互连的网络在数据链路层以上采用相同的协议。

2）网桥的构成，如图 1-68 所示。

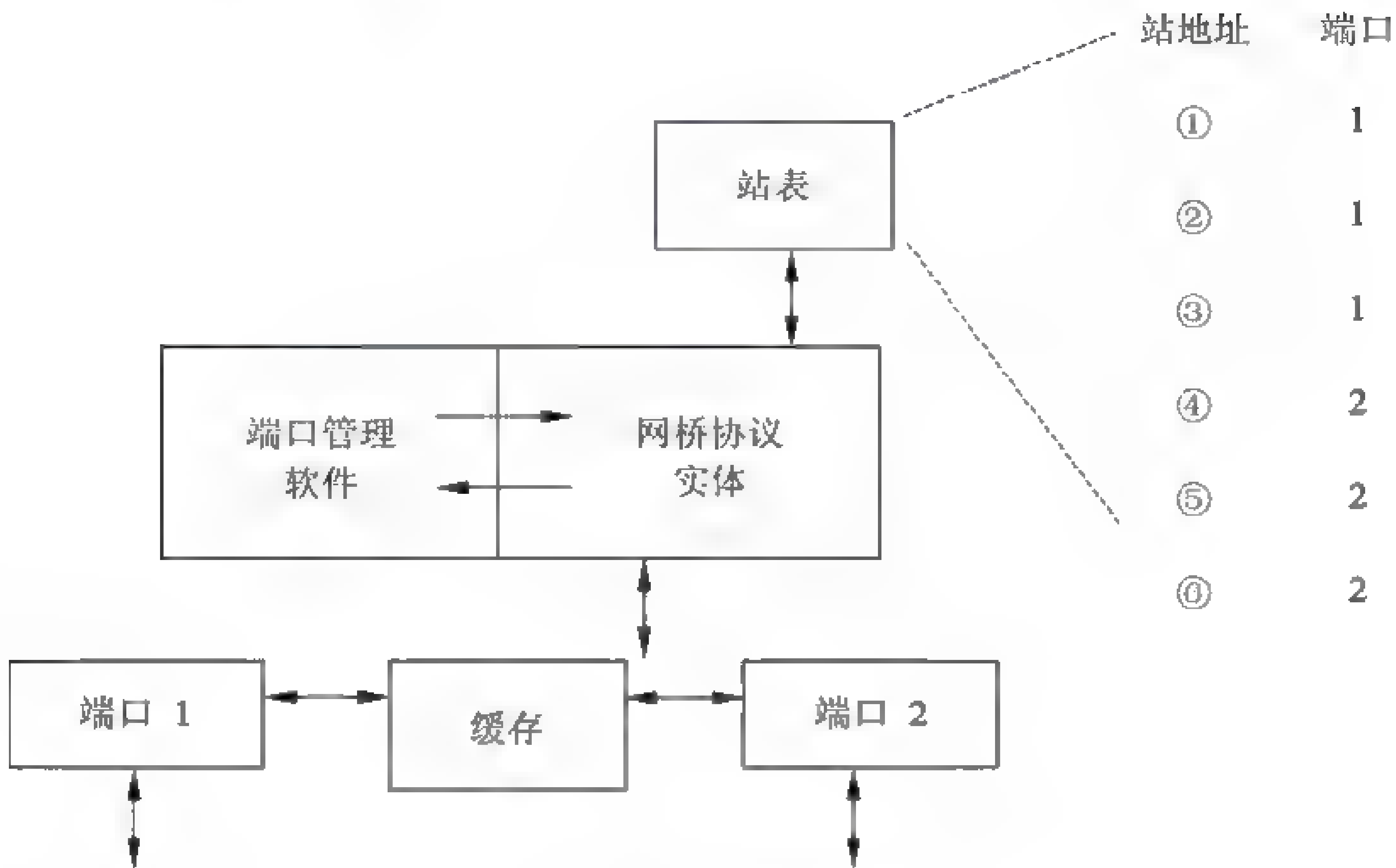


图 1-68　网桥的组成

3）网桥的工作原理

如图 1-69 所示，如果局域网 1 中地址为 201 的节点想与同一局域网中地址为 202 的节点通信，网桥就可以接收到发送帧，但网桥在进行地址过滤后认为不需要转发，因而会将该帧丢弃；如果节点 201 要与局域网 2 中节点 104 通信，节点 201 发送的帧就可以被网桥接收到，网桥进行地址过滤后识别出该帧应发送到局域网 2，网桥将通过与局域网 2 的网络接口转发该帧，这时局域网 2 中的 104 节点将能接收到这个帧。

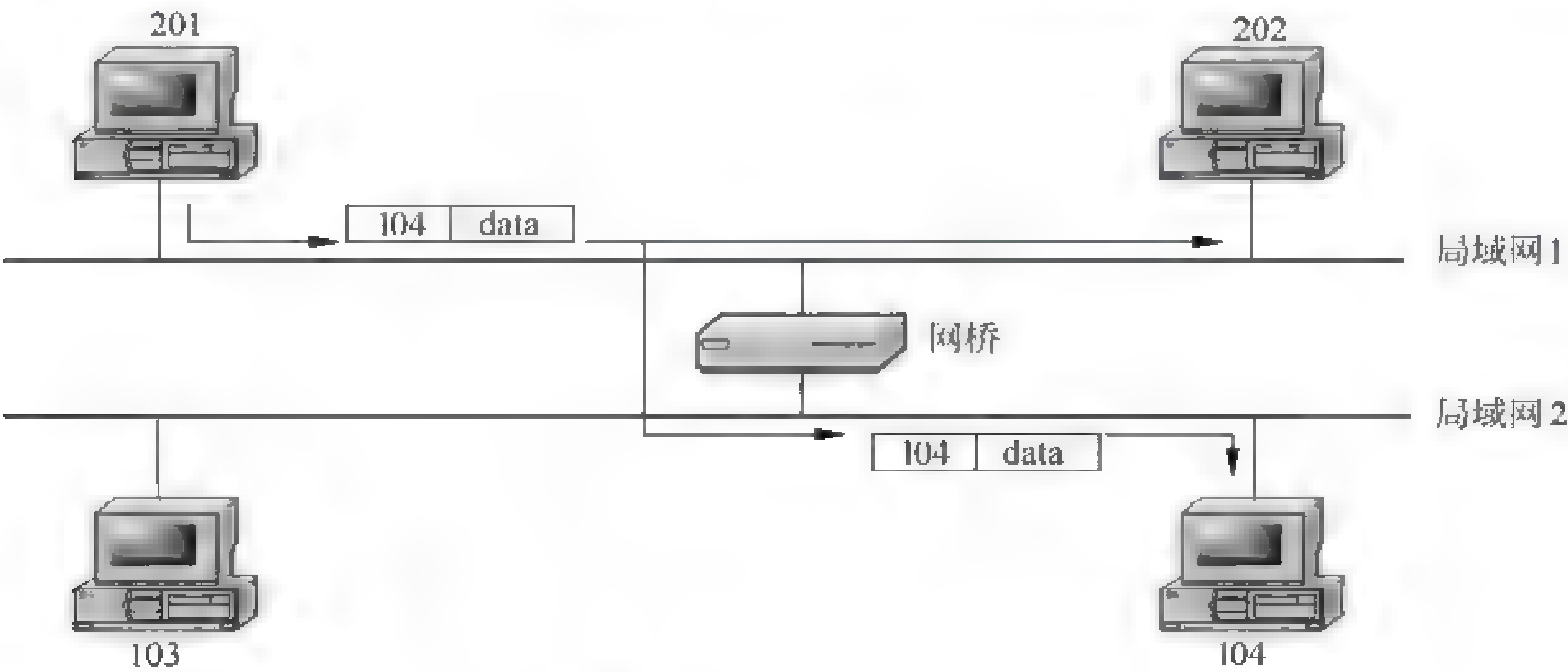


图 1-69　网桥的工作原理

4）网桥的功能

（1）源地址跟踪。

网桥具有一定的路径选择功能，它在任何时候收到一个帧以后，都要确定其正确的传输路径，将帧送到相应的目的站点。网桥将帧中的源地址记录到它的转发数据库（或者地址查找表）中，该转发库就存放在网桥的内存中，其中包括了网桥所能见到的所有连接站点的地址。这个地址数据库是互联网所独有的，它指出了被接收帧的方向，或者仅说明网桥的哪一边接收到了帧。能够自动建立这种数据库的网桥称为自适应网桥。

在一个扩展网络中，所有网桥均应采用自适应方法，以便获得与它有关的所有站点的地址。网桥在工作中不断更新其转发数据库，使其渐趋完备，有些厂商提供的网桥允许用户编辑地址查找表，这样有助于网络的管理。

（2）帧的转发和过滤。

在相互连接的两个局域网之间，网桥起到了转发帧的作用，它允许每个 LAN 上的站点与其他站点进行通信，看起来就像在一个扩展网络上一样。

为了有效地转发数据帧，网桥提供了存储和转发功能，它自动存储接收进来的帧，通过地址查询表完成寻址；然后把它转发到源地址另一边的目的站点上，而源地址同一边的帧就被从存储区中删除。

过滤（filter）是阻止帧通过网桥的处理过程，有三种基本类型：

- 第一种目的地址过滤，当网桥从网络上接收到一个帧后，首先确定其源地址和目的地址，如果源地址和目的地址处于同一局域网中，就简单地将其丢弃，否则就转发到另一局域网上，这就是所谓的目的地址过滤。
- 第二种源地址过滤，就是根据需要，拒绝某一特定地址帧的转发，这个特定的地址是无法从地址查找表中取得的，但是可以由网络管理模块提供。事实上，并非所有网桥都进行源地址的过滤。
- 第三种协议过滤，目前，有些网桥还能提供协议过滤功能，它类似于源地址过滤，由网络管理指示网桥过滤指定的协议帧。在这种情况下，网桥根据帧的协议信息来决定是转发还是过滤该帧，这样的过滤通常只用于控制流量、隔离系统和为网络系统提供安全保护。

（3）协议转换。

早期的 FDDI 网桥结构通常是专用的封装结构，这是由于早期的 FDDI 仅与 IEEE 802.3 或 IEEE 802.5 子网相连，不需要和其他局域网中的节点通信。但是，在一个大型的扩展局域网中，有很多系统在一起操作，这种专用的封装式网桥就无法提供相互操作的能力。为此，采用了新的转换技术，依照与其他网络的桥接标准，形成了转换式网桥，建立可适应局域网互联的标准帧。

5）使用网桥实现 LAN-LAN

如图 1-70 所示，使用网桥实现局域网互连。

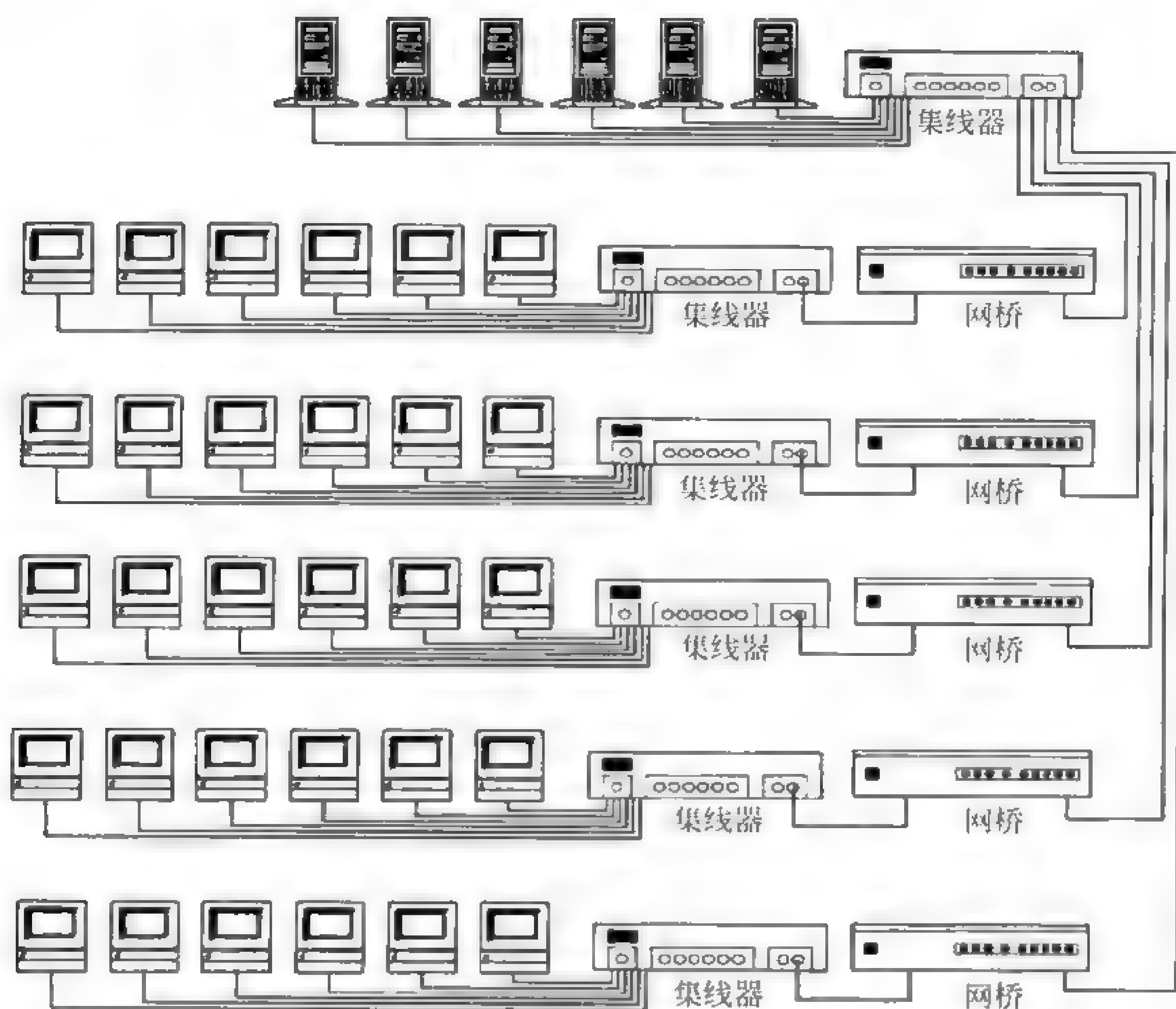


图 1-70　使用网桥实现局域网互连

使用网桥扩展局域网时，所有主机都处于一个广播域上。所以不能使用网桥互连规模较大的网络，以免形成广播风暴。

4．使用交换机扩展局域网

交换机可以看做是高档集线器，有时也被称之为交换式集线器。交换机在同一时刻可进行多个端口对之间的数据传输。每一端口都可视为独立的网段，连接在其上的网络设备独自享有全部的带宽，无须同其他设备竞争使用。所以有时为了提供更快的接入速度，我们可以把一些重要的网络计算机直接连接到交换机的端口上。这样，网络的关键服务器和重要用户就拥有更快的接入速度，支持更大的信息流量。

使用交换机扩展局域网如图 1-71 所示。

传统的交换机本质上是具有流量控制能力的多端口网桥，即传统的（二层）交换机。交换机的工作原理和网桥一样，是工作在链路层的联网设备，它的各个端口都具有桥接功能，每个端口可以连接一个 LAN 或一台高性能网站或服务器，能够通过自学来了解每个端口的设备连接情况。所有端口由专用处理器进行控制，并经过控制管理总线转发信息。

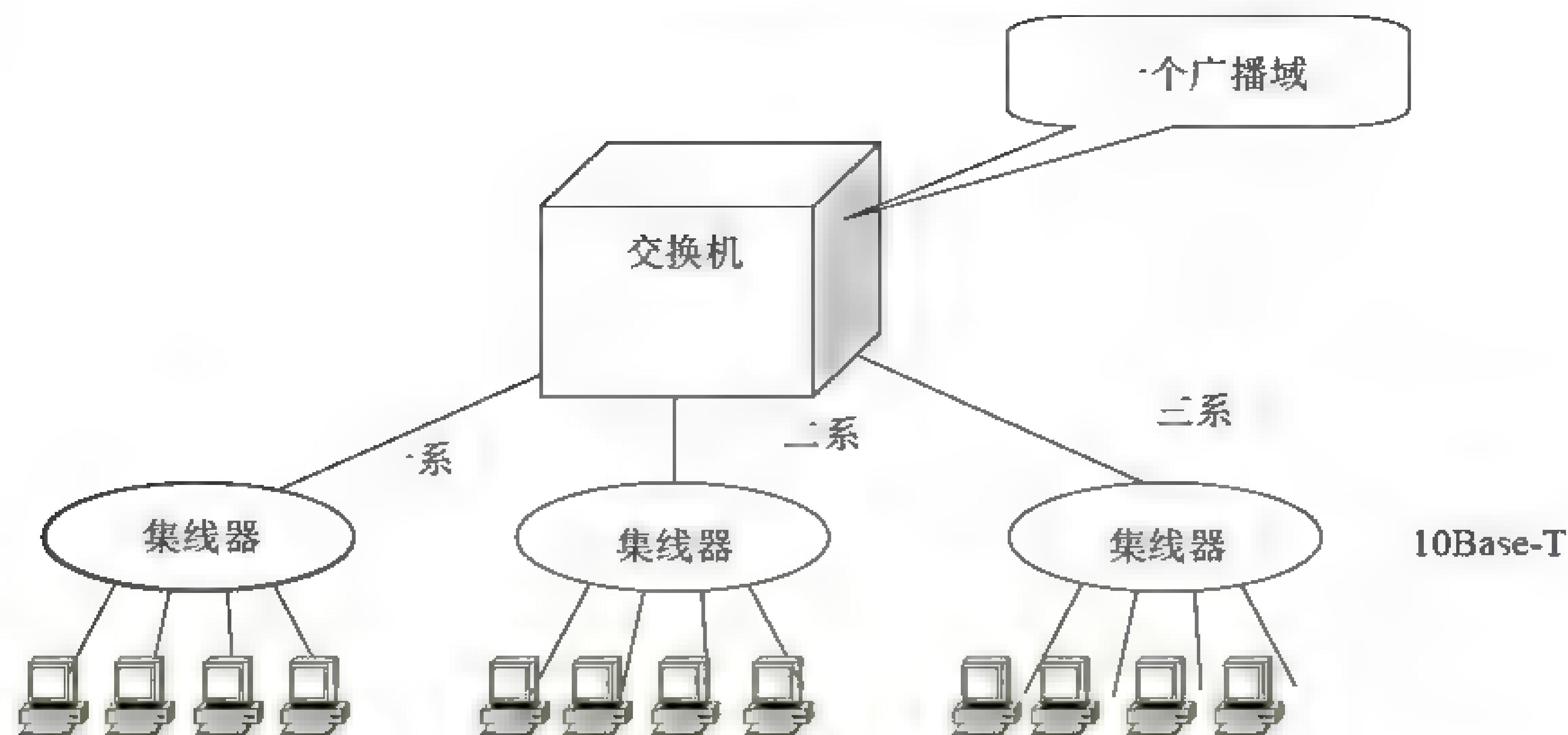


图 1-71　使用交换机扩展局域网

另外，把路由技术引入交换机，可以完成网络层路由选择，故称为三层交换，这是交换机的新进展。

通常把由交换机作为中心设备的局域网称为交换式局域网，如图 1-72 所示。

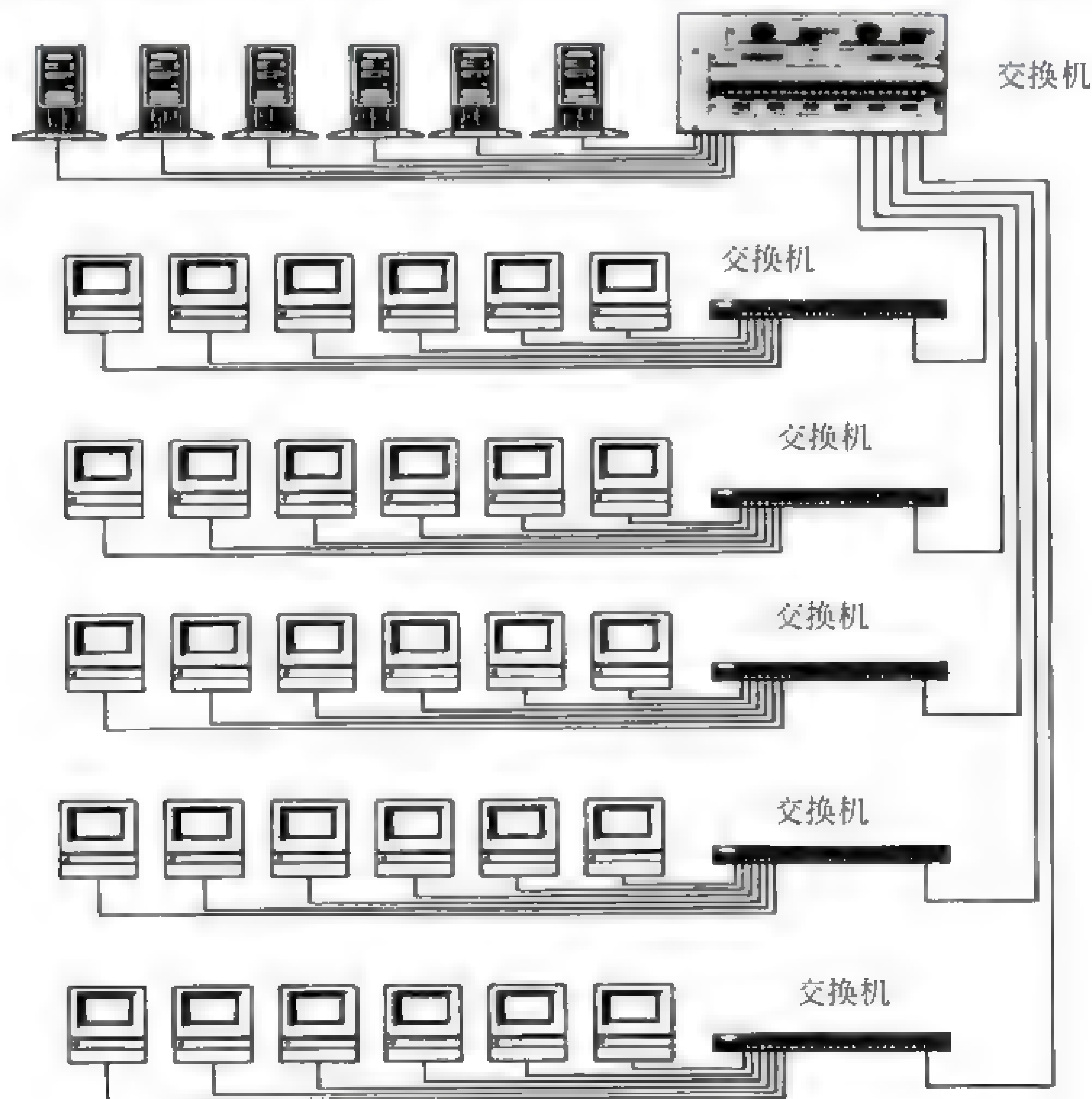


图 1-72　交换机实现局域网内部互连

5. 使用路由器实现 LAN-LAN

路由器对网络进行物理分段的方式与交换机和网桥相同，但它还可以生成逻辑网段。路由器不对广播进行转发。所以通过路由器可以形成更多的广播域或逻辑网段，从而提高网络的性能。如图 1-73 所示，应用路由器实现局域网互连。

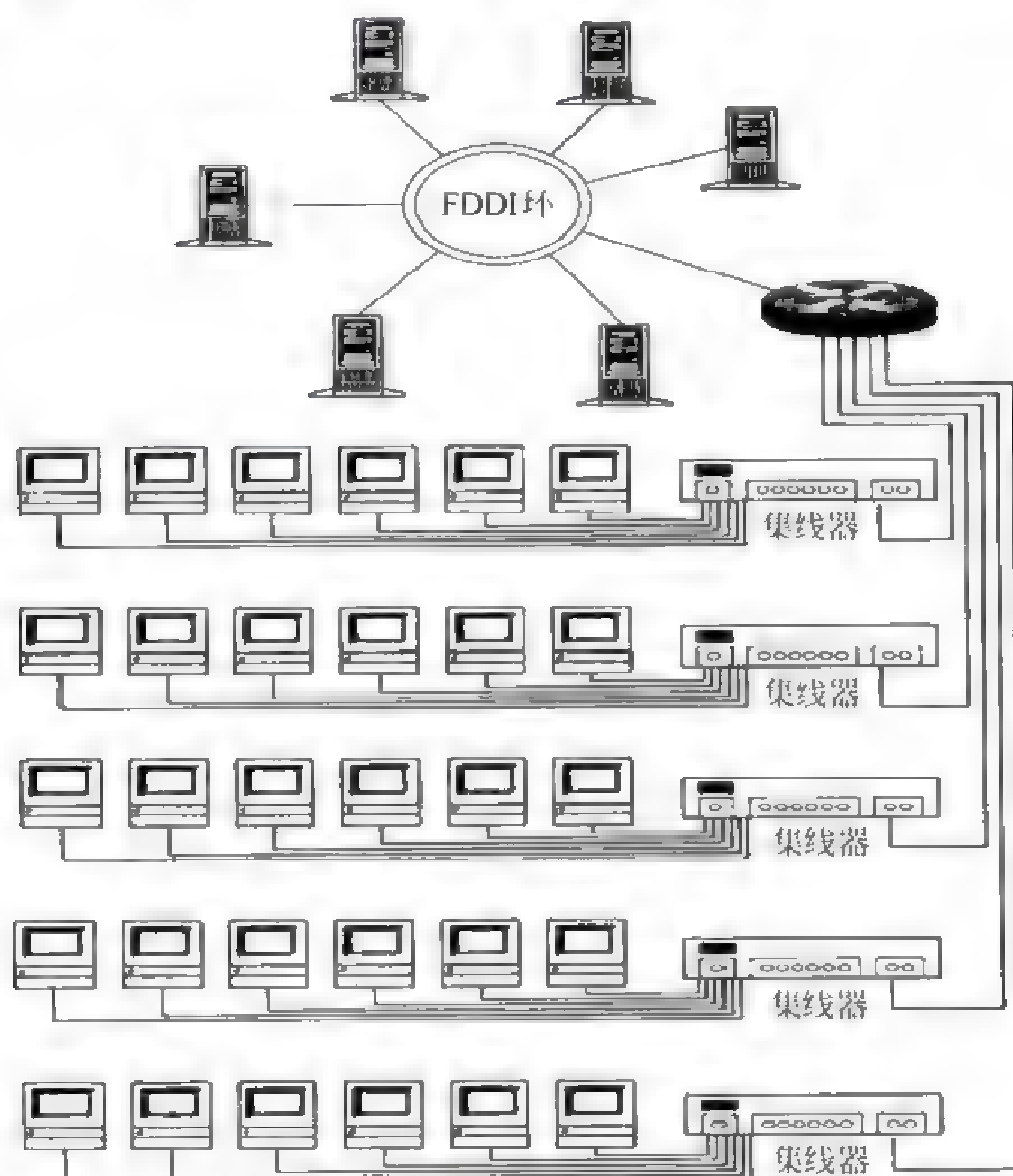


图 1-73　路由器实现局域网互连

另外，如果互连的局域网高层采用了不同的协议，就需要用多协议路由器（如图 1-74 所示）。多协议路由器具有处理多种不同协议分组的能力，它可以处理不同的分组的路由选择与分组转发问题。为了解决互联局域网中不同类型主机之间的通信问题，可以采用多协议路由器的互连结构。

1.7.2.2　LAN-WAN

LAN-WAN 的互连发生在网络层。LAN-WAN 的互连设备是路由器。

路由器是工作在 OSI 参考模型第三层——网络层的数据包转发设备。路由器通过转发数据包来实现网络互连。虽然路由器可以支持多种协议（例如 TCP/IP、IPX/SPX、AppleTalk 等协议），但是在我国绝大多数路由器运行 TCP/IP 协议。图 1-75 是用路由器

将局域网连至互联网络。图 1-76 使用路由器构建企业网。

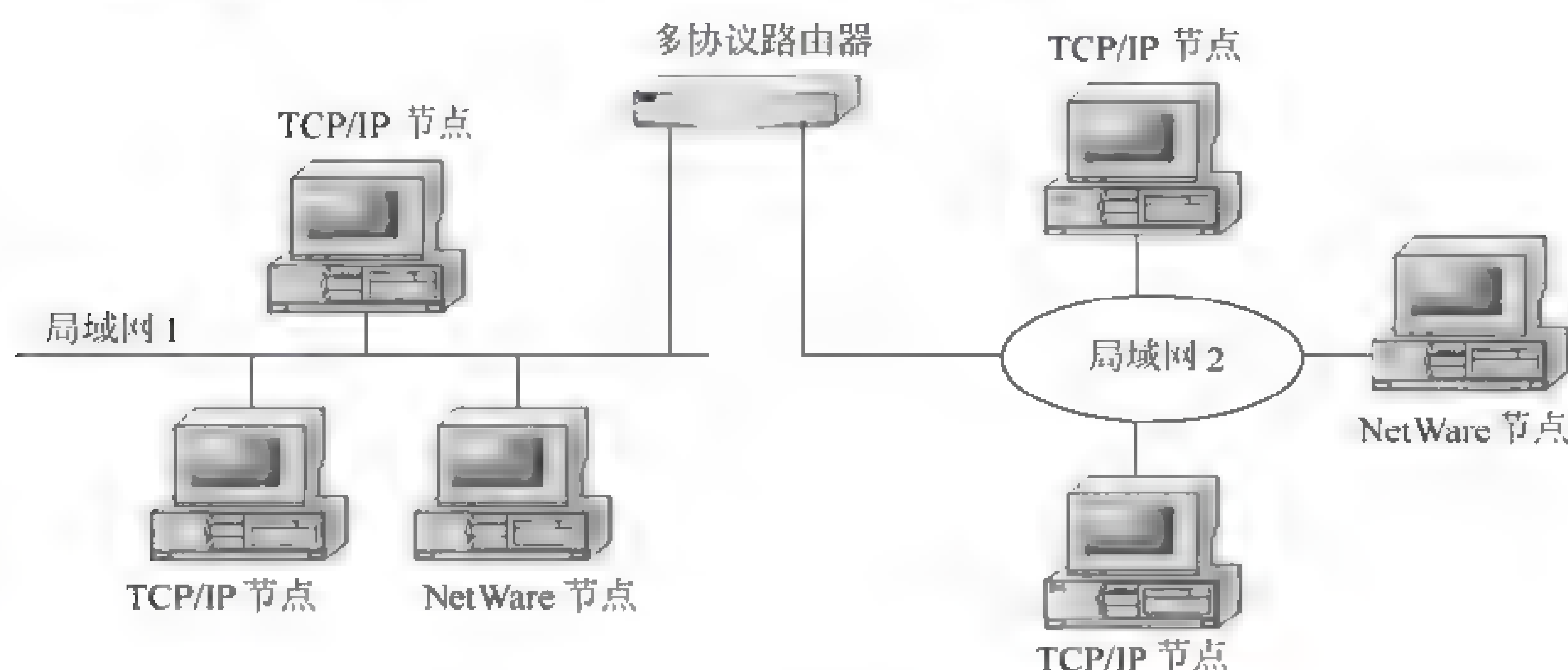


图 1-74 使用多协议路由器实现局域网互连

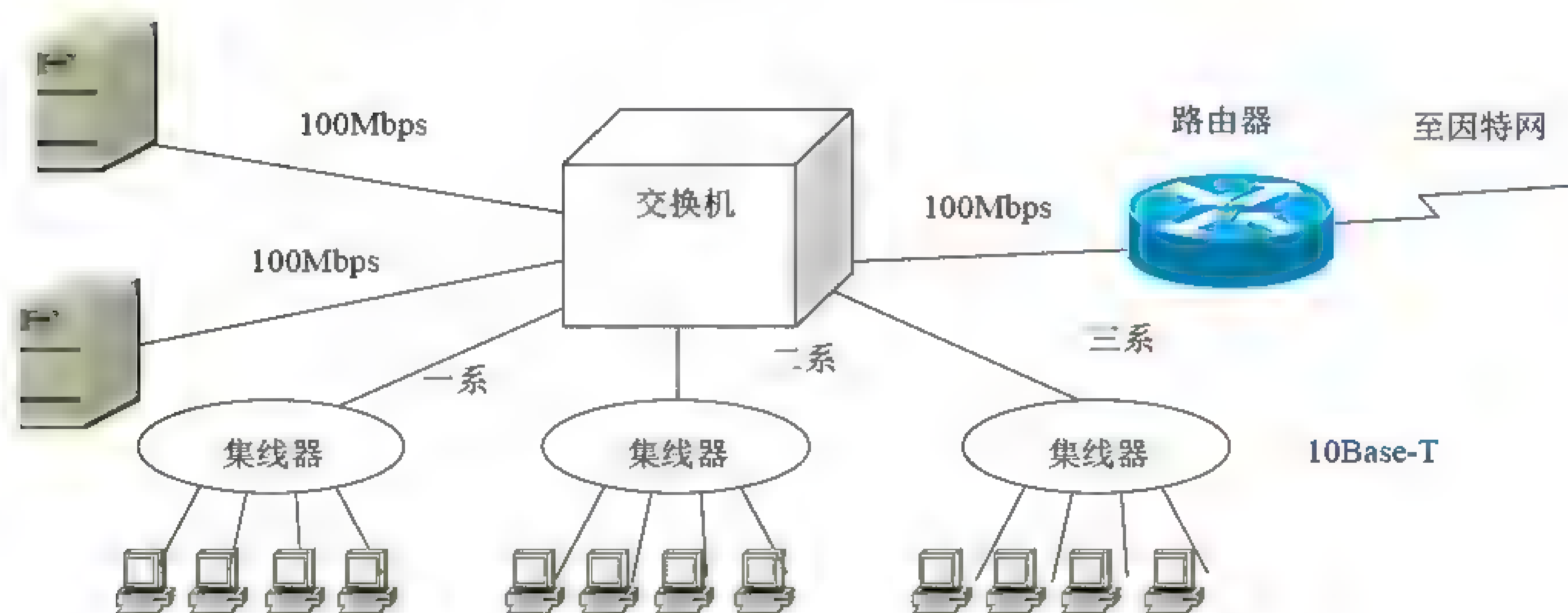


图 1-75 用路由器将局域网连至互联网

1.7.2.3 WAN-WAN

WAN-WAN 互连发生在 OSI/RM 的传输层及其上层。 WAN-WAN 的互连设备是网关，如图 1-77 所示。

网关用于以下几种场合的异构网络互连：

（1）异构型局域网，如互联专用交换网 PBX 与遵循 IEEE 802 标准的局域网。

（3）局域网与广域网的互联。

（3）广域网与广域网的互联。

（4）局域网与主机的互联（当主机的操作系统与网络操作系统不兼容时，可以通过网关连接）。

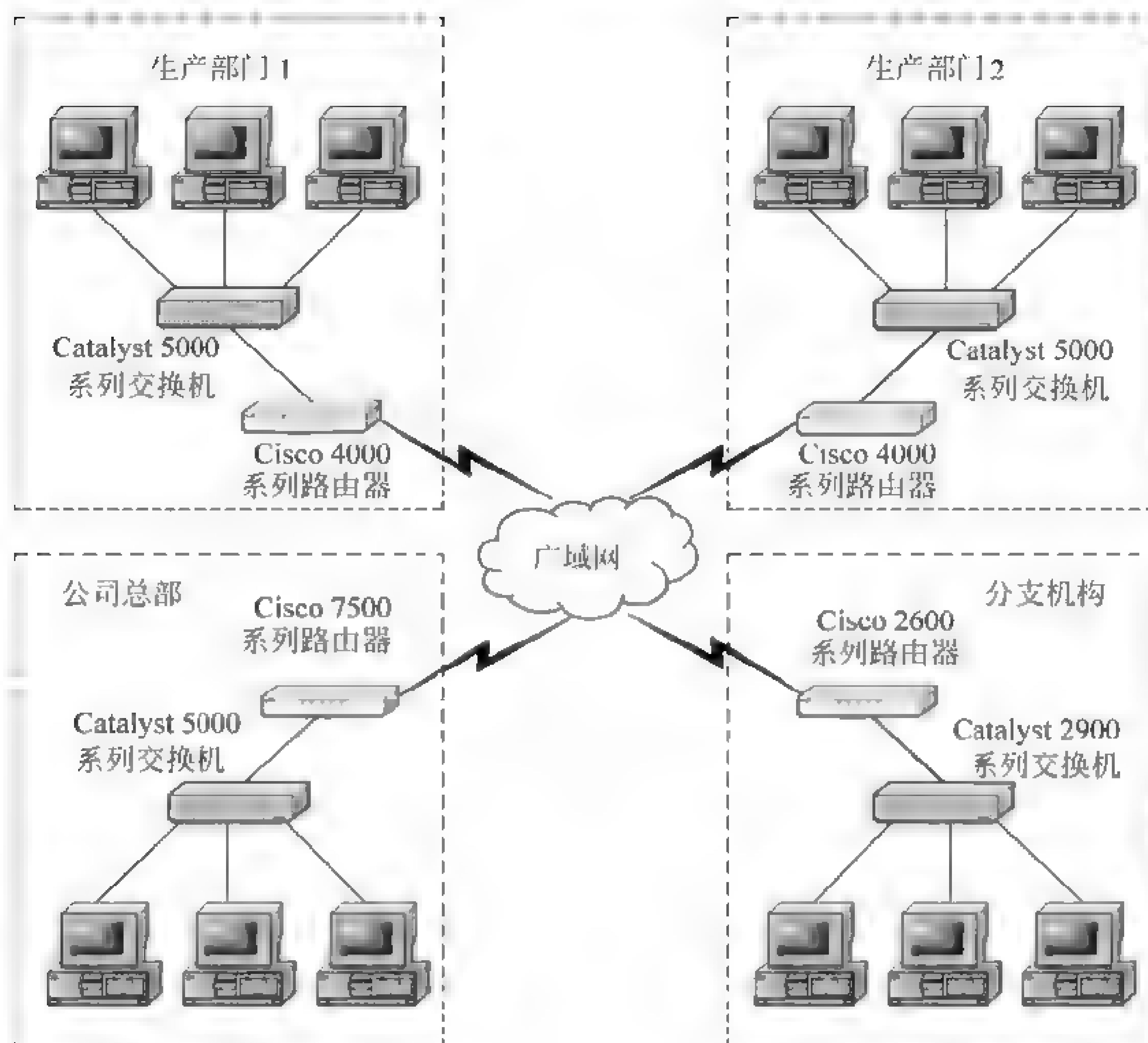


图 1-76 使用路由器构建企业网

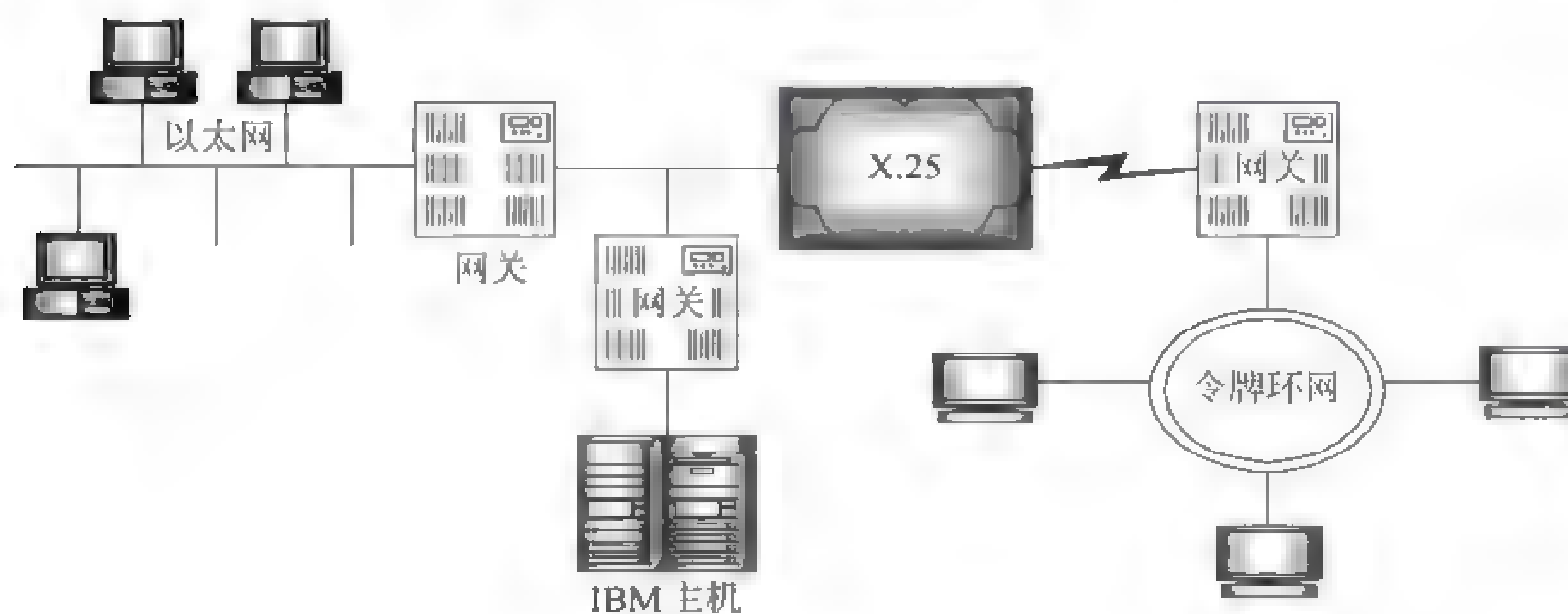


图 1-77 网关互连网络

1.7.3 路由选择算法

路由选择是指通信子网在传输数据包时，在源节点和目的节点之间的多条路由中，以什么规则确定哪条作为转发数据包的通路的问题。路由选择算法是实现路由选择功能

的一些方法。通俗地讲，路由就是将数据包从一个节点转发到另一个节点的一个中继过程，路由功能即是学习和维持网络拓扑结构知识的机制。除了采用广播通信方式外，所有网络都需要具备路由选择功能。路由选择问题是研究和设计计算机网络的关键问题。

不同的网络对路由选择算法的要求不一样，如军用网络要求可靠，普通商用网络要求经济，实时网络要求快速。但不论是什么网络，其路径选择算法都应满足一些基本要求，包括以下特性。

- 正确性：路径选择算法应能使数据包迅速、正确地传送。
- 简单性：算法应尽量简单，易实现，开销小。
- 健壮性：算法能适应网络拓扑结构及流量的变化，在外部条件发生变化时仍能正确地完成要求的功能。
- 可靠性：不管运行多长时间，均应保持正确。例如计数器必须要有足够的位数等。
- 公平性：各节点具有均等的发送信息的机会。

评价路径选择算法优劣的标准会因用户的不同而有所不同。总的来说，路径选择算法最好能找到一条从源节点到目的节点的最优路径。对最优的定义可能是经过的节点数最少、经过的传输距离最短、占用的系统带宽最少、所用的传输时间最短等等。不论是什么标准，都可对最优路径作如下断言：如果节点 X 是从节点 I 到节点 J 的最优路径上的一个节点，那么该路径上从 X 到 J 的那段路径也必然是从 X 到 J 的最优路径。该断言称为最优化原则。为说明最优化原则的正确性，假定从 I 到 X 的路径为 r1，从 X 到 J 的路径为 r2，并假定 r1r2 为最优路径。如果从 X 到 J 有一条比 r2 更好的路径 r2′，则路径 r1r2′应比 r1r2 更好，这与 r1r2 为最优路径相矛盾，故 r2 必为从 X 到 J 的最优路径。

应当指出，因为路由选择是在网络中的节点相互交换信息，共同协作的条件下完成的，所以路由选择是一个非常复杂的问题。另外，网络环境的不断变化、突发问题的出现，这些都是事先无法预料的，这给路由选择也带来了不少困难。此外，当网络发生拥塞，特别需要有好的路由选择算法能缓解这种情况时，又因为这时很难从网络中的各个节点获得所需的路由选择信息，而很难处理。

按照路径选择算法的实现方法，可将其分为静态路径选择算法与动态路径选择算法两大类，后面分别加以介绍。

1．静态路由选择算法

从路由选择算法能否随网络的通信量或拓扑结构自适应地进行调整，可以将路由选择算法分为非自适应路由选择算法和自适应路由选择算法。非自适应路由选择算法也叫静态路由选择算法，它的特点是算法简单、开销较小，但性能差、效率低。非自适应路由选择算法分为以下几类。

1）固定路由算法

这种方法是在每个节点上保持一张路由表，表上标明对每一个目的地址应走哪条链路进行转发。这些表是在整个系统进行配置时生成的，并且在此后的一段相当时间保持

固定不变。当网络拓扑固定不变并且通信量也相对稳定时，采用固定路由法是最好的。

那么如何制作这样的路由表呢？常用的方法是将网络内任何两个节点之间的最短通路事先计算好，然后根据这些最短通路制成路由表，存放在各个节点中。每一个分组都可在所到达的节点中查找到下一步应转发到哪一个节点（即下一个节点或后继节点）。可见这种路由选择策略的关键就是要算出给定网络中任意两个节点之间的最短通路。

下面介绍求最短通路的算法，这是由 Dijkstra 提出的。已知条件是整个网络拓扑和各链路的长度。

应注意到，若将已知的各链路长度改为链路时延或费用，这就相当于求任意两节点之间具有最小时延或最小费用的通路。因此，求最短通路的算法具有普遍的应用价值。

2）分散通信量法（traffic bifurcation）

这种方法事先在每个节点的内存中设置一个路由表，但此路由表中给出几个可供采用的输出链路，并且对每条链路赋予一个概率。当一个分组到达该节点时，此节点即产生一个 0.00～0.99 的随机数，然后按此随机数的大小，查表找出相应的输出链路。

3）洪泛法（flooding）

这种方法是当某个节点收到一个不是发给它的分组时，就向所有于此节点相连的链路转发出去。当然，不能再把这个分组发到它刚刚离开的那个节点，否则就永远有一些分组来回不停地在各条链路上“振荡”。当网络的通信量很小时，洪泛法可使分组的时延为最小。此外，在许多条并行发送的路由中，显然会有一条是最佳的。

实际上在运行网络中却很少采用洪泛法。这是因为采用洪泛法后，网络中的分组数目会迅速增长，结果导致网络出现拥塞现象。

可以采用两种方法来限制分组的数目。一种方法是在每个分组的首部设置一个计数器。每当分组到达一个节点时，计数器即自动加 1。当计数器所计的数到达规定值时（如达到端到端所能达到的最大段数），即将此分组丢弃。另一种方法是在每个节点建立一个登记表，凡经过此节点的分组均进行登记。当某个分组再次通过节点时，即将该分组丢弃。当然，这种方法所付出的代价是各节点都要用去不少的存储空间。建立登记表的方法可以有效地防止分组在网内无限制地循环。

洪泛法在军用网中很有用，因为它有很好的稳健性。洪泛法还可以修改成有选择的洪泛法，它的特点是仅在满足某些事先确定的条件的链路上转发分组，因此分组不会向不希望去的方向转发。

4）随机走动法（random walk）

这种方法又称为随机徘徊，其特点是当分组到达某个节点时就随机地选择一条链路作为转发的路由。例如，某节点可供转发的输出链路共有 3 条，那么就以平均概率 0.33 选择任一条链路作为其转发的路由。在非自适应的路由策略中，若可能发生节点或链路的故障，那么随机走动法已被证明是非常有效的，它使得路由算法具有较好的稳健性。

2. 自适应路由选择算法

上述静态路由选择算法都只考虑了网络的静态情况，且主要考虑的是静态拓扑结构。在一个实际的网络中，网络节点众多，随时都有节点开始或停止工作，网络的拓扑结构随时都有可能发生变化，同时各节点的通信请求也是不可预知的，网络上的负载状况也是动态变化的，因而采用静态路由选择算法一般不能很好地满足路由选择的基本要求，甚至根本就不能找到一条路由。因此研究既考虑拓扑结构又考虑通信负载的动态路由选择算法就十分必要。

动态路由选择算法也叫自适应路由选择算法，它的特点是能较好地适应网络状态的变化，但实现起来比较复杂。其工作过程包括以下 4 个部分。

- 测量：测量并感知网络状态，主要包括拓扑结构、流量及通信延迟。
- 报告：向有关进程或节点报告测量结果。
- 更新：根据测量结果更新路由表。
- 决策：根据新路由表重新选择合适的路由转发数据包。

1）孤立自适应路由选择算法

这类算法只根据本节点获知的网络信息确定数据包的输出线，节点之间不交换路由信息。

（1）热土豆算法。

在网络中，每条输出线都有若干缓冲区，供等待输出的数据包排队使用。热土豆算法的思想是，每收到一个数据包，总是选择队列最短的输出线转发数据包，以求最快输出。其名字的由来是缘于当人拿到一个热土豆时，因害怕手被烫伤，总想尽快地将其丢出去。

热土豆算法在转发数据包时，只考虑了队列的长度即包的数量，没有考虑网络的带宽及全网的负载状况。当网络每部分的带宽不一样时，该算法不能保证转发的路径是最优路径。

（2）反向探知算法。

当一个节点首次转发要到达某一节点的数据包时，由于此前没有进行过相应的路径选择，因而要选择一条到该节点的路径并不是一件简单的事。但是本节点先前转发过某些数据包，记录着目前要转发的数据包中的目的节点到源节点的信息，即当前数据包的反向路径，则本节点就可利用该信息，试探着沿原路径的反向路径转发数据包。反向探知算法就是采用这种方法来寻找路径的。

反向探知算法的明显缺点是：① 路径信息是间接的，不可靠的；② 当没有反向路径信息时，正常的路径选择就难以完成；③ 存在来回传送即振荡的可能。

2）分布式路由选择算法

在分布式路由选择算法中，最基本的算法有两个，即距离向量路由选择算法和链路状态路由选择算法。

（1）距离向量路由选择算法。

在距离矢量路由选择算法中，每个路由器维持有一张子网中每一个以其他路由器为索引的路由表，表中每一个项目都对应于子网中的每个路由器。此表项包括两个部分，即希望使用的到目的地输出线路和估计到达目的地所需时间或距离。所用度量标准可分为站点，估计的时间延迟（ms），该路由排队的分组估计总数或类似的值。

假定路由器知道它到每个相邻路由器的“距离”。如果度量标准为站点，其距离就为一个站点。如果度量标准是队列长度，则路由器会简单地检查每个队列。如果度量标准是延迟，路由器可以直接发送一个特别“响应”分组来测出延迟，接收者只对它加上时间标记后就尽快送回。

例如，设某节点 J 经相邻节点 Y，J 的相邻节点为 X_1，X_2，…，X_n。则 J 需要选择输出线（X_1，X_2，…，X_n）之一进行转发。选择前先计算延迟时间：

$$T_{JY\min}=\min\{t_{JX1}+T_{X1Y},\ t_{JX2}+T_{X2Y},\ \cdots,\ t_{JXn}+T_{XnY}\}$$

式中，t_{JX1}，t_{JX2}，…，t_{JXn} 是当前已知数值；T_{X1Y}，T_{X2Y}，…，T_{XnY} 是各相邻节点到目的节点的延迟，通过交换信息后得到的值。找出 T_{JY} 最小的一条路径，如 X_i，然后转发。

该算法在理论上能有效工作，但实现是有诸多缺点，主要有如下三个方面：

第一，无穷计算问题。其中突出的问题是爱好听好消息，即对好消息反应快，对坏消息反应慢。例如，对于图 1-78 所示的网络，开始时 A 与 B 未连接，此时当 B 要向 A 发送信息时，无法完成。在某时刻，A 与 B 连通，交换信息时，C 得知它可以到达 A，距离为 2。以后 D，E 依次得知分别有距离为 3，4 的路径到达 A。B 很快就获知到 A 的路径。这是好消息。若在某个时刻，A 与 B 断开了（可能是下网或 A，B 间线路断开），这时 B 不能直接与 A 通信，但知道 C 与 A 间有通路，于是将信息发送给 C，由 C 转发；C 通过 B 无法转发，又会通过 D 转发，依此类推，直到经若干次交换信息，E 报告与 A 无法通信。这时 B 才断定与 A 不能通信。对这一坏消息，网络反应很慢。事实上是在测试了所有可能性后才知道，因为各节点间交换路径和延迟信息是逐步进行的。当网络很大时，这个过程是缓慢的。在这个例子中采用的测量标准是站点数，它存在一个上限值，容易判断什么时候停止测试。但是如果改用延迟时间作为测量标准，因为上限值无法确定，因而终止条件难以确定，只得让算法一直测量或等待下去。这就是无穷计算的原因。

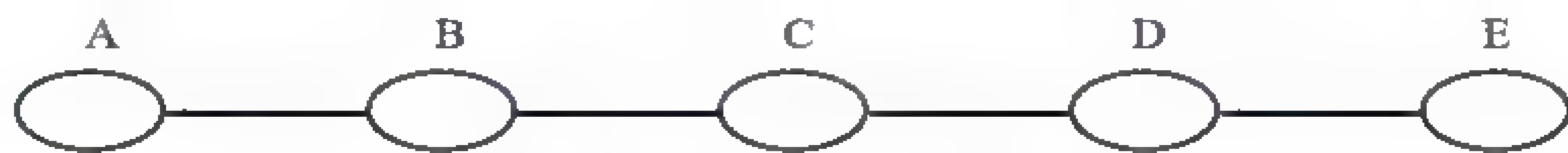


图 1-78　无穷计算问题

第二，开销大。每个节点不仅要计算大量数据，而且还要周期性地与邻节点交换信息，增加大量通信开销。

第三，可能造成阻塞。由于网络的延迟及路径信息的传播是通过相邻节点间交换信息实现的，而这一过程是按周期分布完成的，使得网络中各节点获知网络状态的时间有

先有后，从而影响路径选择，导致大量数据包选择了先前是较优路径，而当前已不再是较优甚至是不通的路径转发，最终导致网络阻塞。

（2）链路状态路由选择算法。

在距离向量选择算法中，有两个主要问题没有得到解决。一是在延迟度量标准中没有考虑网络的带宽。早期的网络比较简单，各部分带宽是一致的，但现在网络已变得十分复杂，各部分性能可能相差甚远，带宽已是一个不可忽视的因素；二是开销问题。算法用于记录、传递延迟和路由信息的时间和资源开销随着网络规模的扩大而变得十分严重，必须加以解决。链路状态路径选择算法就是对距离向量算法的一种改进。

在链路状态路径选择算法中每个节点的工作可以分为如下 4 部分：

- 发现邻节点，并知道其地址。
- 测量到各邻节点的延迟。
- 将所测量到的信息告诉其他节点。
- 重新计算路由。

每一部分的具体功能如下：

① 发现邻节点。

任何节点工作时，都必须知道邻节点。其方法是向每个链路发送一个特殊的信息包，由链路另一端的节点回送一个应答包，节点据此知道邻节点是谁。

② 测量到邻节点的延迟。

发送一个特殊的测量包到各相邻节点，各相邻节点收到该包后，必须立即给以应答。待收到应答后用所需时间除以 2 作为到相应节点的延迟。在测量延迟时，可考虑带宽因素对延迟的影响。为此，一种方法是，测量多次，然后取平均值作为延迟，但在一个巨型网络中，一般不这样做；另一种方法是，测量延迟时把所有的时间开销，如等待时间全部计算在内，这样一般能更真实地反映网络的状态。但这样做的缺点是，可能造成振荡，即在多条路径中在某个时刻一条路径延迟小，使得全部包都选择该路径，导致该路径堵塞，再测量时发现另外路径延迟小，所有包又选择到另外路径，使系统来回更换路径，即形成振荡，却不能均匀地分配这些通信载荷到各路径上。

③ 报告测量结果。

当一个节点测量到所有邻节点及延迟信息后，就用一个特殊的包（称为链路状态包）将测量的结果通知邻节点。

链路状态包的传送对算法的运行有着重要影响。因为，如果链路状态包以不同的延迟到达邻节点，或部分包丢失，就可能导致各邻节点会使用不同版本的信息，而这些信息可能对应着不同的网络拓扑结构，从而可能导致路径的不一致性、死循环、不可到达的节点及其他问题出现。链路状态包通常采用广播或扩散的办法传送。链路状态包中应包括一个序号，以区别不同的链路状态包。邻节点收到该包后，根据序号作相应处理。若该包已收到过，就丢弃；否则，记录该包并进行扩散。该方法存在一个问题，就是某节点在工作过程中因故复位，重新工作后序号从头开始，使得其他节点本来是新包当成了接收过的旧包而丢弃掉。

④ 重新计算路由。

每个节点周期性地收到其他节点发送的链路状态包后，就可以周期性地重构网络拓扑，并且可以知道任意两个相邻节点之间的延迟时间，节点根据这些信息就可以使用 Dijkstra 算法重新计算到达任意节点的最优路径供下次转发数据包时使用。

链路状态路径选择算法是曾被广泛采用的一种算法，如 NSFNET、Netware、DecNet、OSPF 等都使用过该算法。

3．广播路由选择算法

对于一些特定的应用，如天气预报、股市行情或电视节目等，一个节点需要将数据发送到其他所有节点。将数据同时发送给所有其他节点的方式称为广播。在有些应用中，一个节点需要将信息发送给网内部分节点，这种方式称为组播或多播（multicast）。

1）广播路由选择算法

实现广播的算法有多种，主要有以下一些。

- 独立发送方法：这种方法不需要子网络具有特殊的广播功能。当需要广播信息时，广播节点采用点对点传送策略将广播信息向每个节点发送一遍。这种方法不仅需要广播节点知道所有节点的地址，而且也非常浪费带宽。在很多小型网络中，这是一种唯一可用的方法，但也是最不理想的方法。
- 扩散方法：扩散方法的显著缺点是，产生太多的重复包，浪费带宽。在扩散方法中，必须采取控制策略，以防产生广播风暴，即大量的包不断繁殖、循环传送。
- 多目的路径选择：该方法是让每个包都包含一张目的地址清单。每个中间节点根据地址清单确定输出线集合，并复制包，制作新的目的地址清单。依此过程，直到到达最后一个节点即目的地址清单为空为止。
- 生成树方法：生成树是子网的子集，包括所有节点，但不包含回路。该方法以源节点作为生成树的根，采用扩散方法转发数据包，是一种高效的实现方法。但问题是每个节点都需要知道相应的生成树。
- 逆向转发方法：该方法近似于生成树方法但不需要事先知道生成树。该方法的基本思想是，当节点收到一个广播包时，就检查该包是否来自通常用于从本节点发送包到广播源的链路。若是，则此广播包极可能是从源节点来的第一个包，这时，本节点复制该包并将其从输入线外的所有链路转发；如果该广播包不是来自从本节点到达广播源的链路，即输入线不是从本节点到广播源的路径的初始输出线，就丢弃该包。

2）组播路由选择算法

为了实现组播，每个节点都需要知道自己属于哪个组，同时需要计算一棵覆盖整个子网的生成树。在转发过程中，对生成树进行修剪，去掉那些不能到达小组成员的线路，最终得到一个只包含小组成员的生成树。

4．分层路由选择算法

随着网络的增大，路径选择表会急剧增大。这些表格不仅占用大量存储器空间，更严重的是，测量、计算、交换网络状态及路径信息会占用大量的时间。当网络节点数达

到一定规模后，再以节点为单位进行路径选择已变得不可能。层次路径选择算法就是针对这一情况而采取的解决方法。

层次路径选择算法也叫分级路径选择算法，其基本思想就是先将网络分成区域，将区域分成簇，再将簇分成区，区分为组，直到最后每个单位内节点数较少为止。具体分多少层，要视网络的规模而定。在进行路径选择时，在每一层上，都以该层的划分单位作为一个虚拟节点进行路径选择，当包到达该虚拟节点后，再以下级划分单位进行路径选择，直到最后到达实际的目的节点为止。例如，在第一层，以区域为单位进行路径选择，而区域数可能较少，实现起来相对容易，到达一个区域后，再以簇为单位进行路径选择。依此类推。如对于因特网，可将一个国家分为一个区域，这样在顶层就只有 100 多个虚拟节点，在每一个国家(区域)内，根据规模大小可进一步分成簇、区、组等。如在中国某处的一个节点要向美国的某节点发送信息，当进行路径选择时，不是直接找到达对方节点的路径，而是先找到达美国的路径。到达美国之后，路径由位于美国的节点依据相同的算法完成。

层次路径选择算法在每一层上的选择算法可采用前面已经介绍的方法实现。层数的多少，对路径选择的效率、性能会有不同的影响。Kamoun 和 Kleinrock 已证明，对于 N 个节点的网络，最优层数为 lnN，每个节点需要的表项总数为 e lnN。

1.8 Internet 协议

Internet 协议的主要协议及其层次关系如图 1-79 所示。

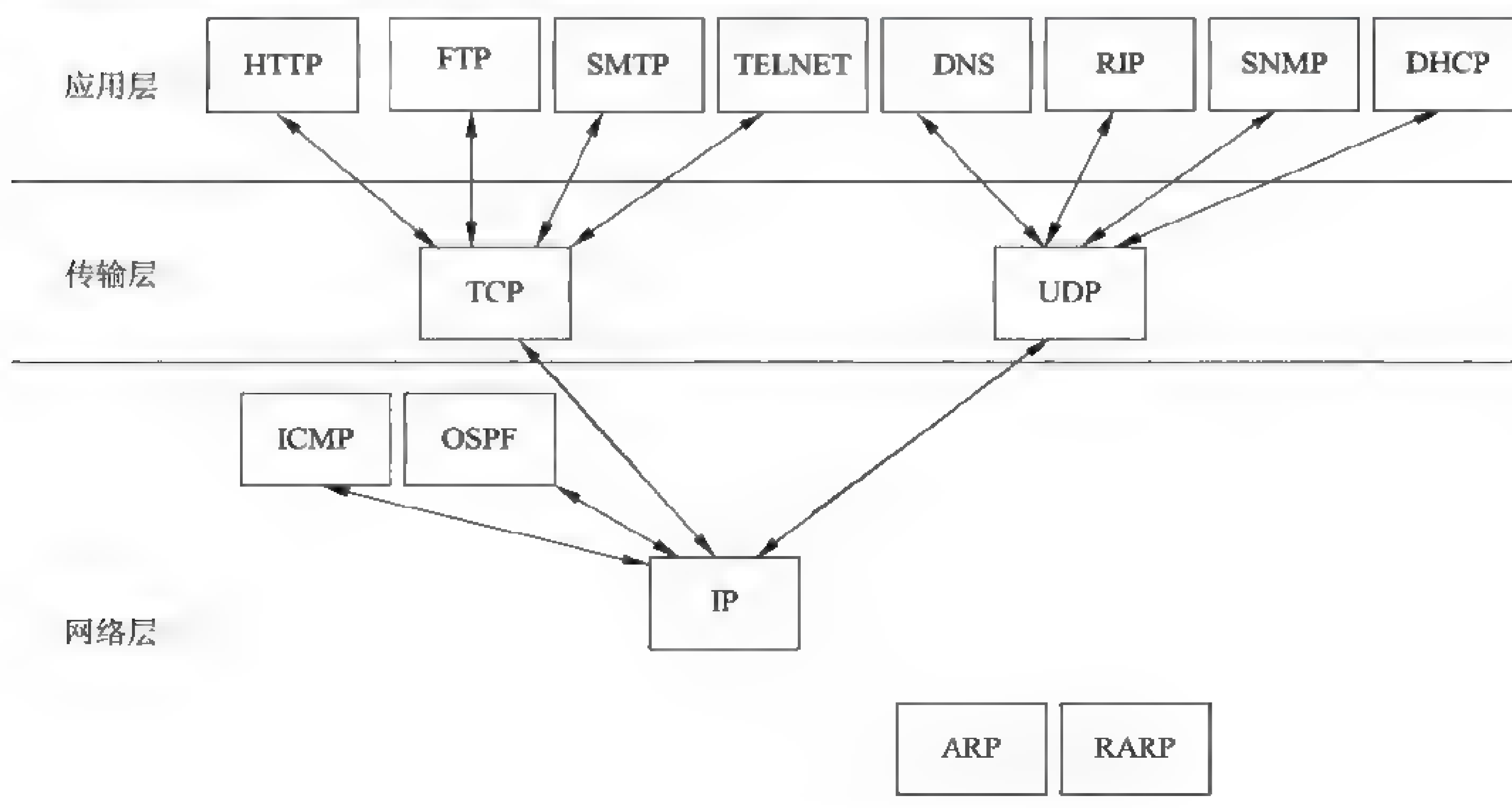


图 1-79 Internet 协议及其层次关系

1.8.1　网络层协议

1.8.1.1　IPv4 协议

1．IP 地址

1）概述

Internet 中有数百万台以上的主机和路由器，IP 地址可以确切地标识它们。一台主机至少拥有一个 IP 地址。任何两台主机的 IP 地址不能相同，但是允许一台主机拥有多个 IP 地址。如果一台计算机虽然也连入 Internet，使用 Internet 的某些功能，但它没有自己的 IP 地址，就不能称为主机。它只能通过连接某台具有 IP 地址的主机实现这些功能的，因此只能作为上述主机的仿真终端，其作用如同该主机的普通终端一样，而不论其自身的功能有多强。

IP 地址的划分经过了三个阶段：分类的 IP 地址；子网的划分；构成超网。

2）分类 IP 地址结构及类别

IP 地址是由 32 位二进制数，即 4 个字节组成的，它与硬件没有任何关系，所以也称为逻辑地址。它由网络号和主机号两个字段组成，这样的 IP 地址是两级 IP 地址，如图 1-80 所示。IP 地址的结构使我们可以在因特网上很方便地进行寻址，这就是：先按 IP 地址中的网络号（net-id）把网络找到，再按主机号（host-id）把主机找到。所以 IP 地址并不只是一个计算机的代号，而是指出了连接到某网络上的某计算机。



图 1-80　IP 地址结构

为了便于对 IP 地址进行管理，同时还考虑到网络的差异很大，有的网络拥有很多主机，而有的网络上的主机则很少。因此因特网的 IP 地址分成为 5 类，即 A 类到 E 类，如图 1-81 所示。目前大量使用的 IP 地址是 A，B，C 三类。当某单位申请到一个 IP 地址时，实际上只是获得了一个网络号 net-id，具体的各个主机号由本单位自行分配。

比特	31	23	15	7	0
A 类	0　net-id	host-id			
B 类	10　net-id		host-id		
C 类	110　net-id			host-id	
D 类	1110　组播地址				
E 类	11110　保留为以后使用				

图 1-81　IP 地址的类型

3）特殊 IP 地址

IP 定义了一套特殊地址格式，称为保留地址。这些特殊地址包括网络地址、主机地址、直接广播地址、有限广播地址、本机地址。

4）子网及子网掩码

两级 IP 地址的缺点：

- IP 地址空间的利用率有时很低。
- 给每一个物理网络分配一个网络号会使路由表变得太大因而使网络性能变坏。

在 IP 地址中增加一个 subnet-id 字段，使两级的 IP 地址变成为三级的 IP 地址。这种做法叫作划分子网（subnetting），如图 1-82 所示。划分子网纯属一个单位内部的事情。单位对外仍然表现为没有划分子网的网络。因此子网号 subnet-id 是从两级 IP 的主机号部分“借用”的若干个位。

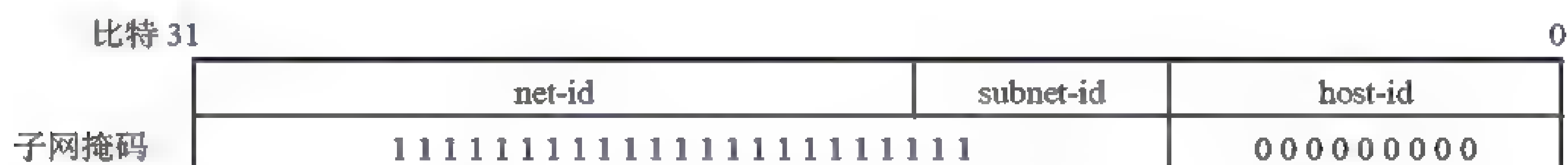


图 1-82 三级 IP 地址的类型及子网掩码

当外面的分组进入到本单位网络后，本单位的路由器如何确定应转发的子网呢？这就是子网掩码的作用。将子网掩码和 IP 地址进行逐位相“与”，所得的结果就是网络地址。这里的网络地址显然是 net-id 和 subnet-id 不变 host-id 全 0 的。

5）VLSM 和 CIDR

在 1992 年因特网面临三个必须尽早解决的问题：

- B 类地址在 1992 年已分配了近一半，眼看就要在 1994 年 3 月全部分配完毕！
- 因特网主干网上的路由表中的项目数急剧增长（从几千个增长到几万个）。
- 整个 IPv4 的地址空间最终将全部耗尽。

1987 年，RFC 1009 指明在一个划分子网的网络中可同时使用几个不同的子网掩码。使用变长子网掩码（Variable Length Subnet Mask，VLSM）可进一步提高 IP 地址资源的利用率。

在 VLSM 的基础上又进一步研究出无分类编址方法，正式名字是无分类域间路由选择（Classless Inter-Domain Routing，CIDR）。

CIDR 两级编址的记法如图 1-83 所示。



图 1-83 CIDR 两级编址结构

CIDR 常采用如 128.14.32.0/20 的表示方法，即在 IP 地址后面加上一个斜线“/”，然后写上网络前缀所占的比特数。并隐含地指出 IP 地址 128.14.32.0 的掩码是 255.255.

240.0。CIDR 虽然不使用子网了，但仍然使用“掩码”这一名词（但不叫子网掩码）。

CIDR 将网络前缀都相同的连续的 IP 地址组成“CIDR 地址块”。即一个 CIDR 地址块可以表示很多地址，这种地址的聚合常称为路由聚合，它使得路由表中的项目大大减少。

另外 IP 地址还分为全球地址和专用地址。RFC 1918 指明的专用地址是：

- 10.0.0.0～10.255.255.255（或记为 10/8）
- 172.16.0.0～172.31.255.255（或记为 172.16/2）
- 192.168.0.0～192.168.255.255（或记为 192.168/16）

2．IPv4 数据报格式

IPv4 数据报格式如图 1-84 所示。

0	4	8	16	19	24	31
版本	首部长度	服务类型	总长度			
标识			标志	片偏移		
生存时间		协议	首部检验和			
源地址						
目的地址						
可选字段（长度可变）					填充	
数据部分						

如图 1-84　IPv4 数据报格式

- 版本：4bit，指 IP 协议的版本，目前的 IP 协议版本号为 4（即 IPv4）。
- 首部长度：4bit，可表示的最大数值是 15 个单位（一个单位为 4B），因此 IP 的首部长度的最大值是 60B。
- 服务类型：8bit，用来获得更好的服务，包括时延、吞吐量、可靠性、路由费用等。在相当长一段时期内并没有什么人使用服务类型字段，直到最近，当需要将实时多媒体信息在因特网上传送时，服务类型字段才重新引起大家的重视。
- 总长度：16bit，指首部和数据之和的长度，单位为字节，因此数据报的最大长度为 65 535B。总长度必须不超过最大传送单元 MTU。
- 标识：16bit，为了使分片后的各数据报片最后能准确地重装成为原来的数据报。
- 标志：3bit，目前只有前两个比特有意义。
- 片偏移：12bit，表示较长的分组在分片后，某片在原分组中的相对位置。片偏移以 8B 为偏移单位。
- 生存时间：8bit，记为 TTL，表示数据报在网络中的寿命，初始值为允许经过的跳数，一般为 15。
- 协议：8bit，指出此数据报携带的数据使用何种协议，以便目的主机的 IP 层将数据部分上交给哪个处理过程。
- 首部检验和：16bit。只检验数据报的首部不包括数据部分。这里不采用 CRC 检验码而采用简单的补码计算方法。

- 源地址：4B。
- 目的地址：4B。
- 可选字段：用来增加 IP 数据报的功能。
- 填充：能够填充 32 位。
- 数据部分：使用 IP 数据报所传输的内容和协议字段有很大的关系。假如协议字段指明是 TCP 协议，那么数据部分就是一个 TCP 报文。但如果 IP 包分片了，就不是一个完整的 TCP 报文了。

3．IP 数据报的封装与分片

IP 数据报处于网络层，在传送时它需要下层协议给它提供服务，把它封装在数据链路层的协议数据单元——帧的数据域中。而数据帧的格式和其数据域大小的定义和上层协议是独立的，它不会事先去考虑上层的协议数据单元的大小。所以如果下层帧的数据域小于 IP 数据报大小，IP 数据报必须分片。如果 IP 数据报传送时进行了分片，IP 首部的“总长度”字段不是指未分片前的数据报长度，而是指分片后每片的首部长度与数据长度的总和。

也就是说 IP 数据报的长度一定不能超过数据链路层的最大传送单元 MTU，即下层帧的数据域的大小。通常以太网的 MTU 为 1500B，PPP 的 MTU 为 296B，FDDI 的 MTU 为 4352B，令牌环的 MTU 为 4464B。图 1-85 说明了 IP 的封装与分片。

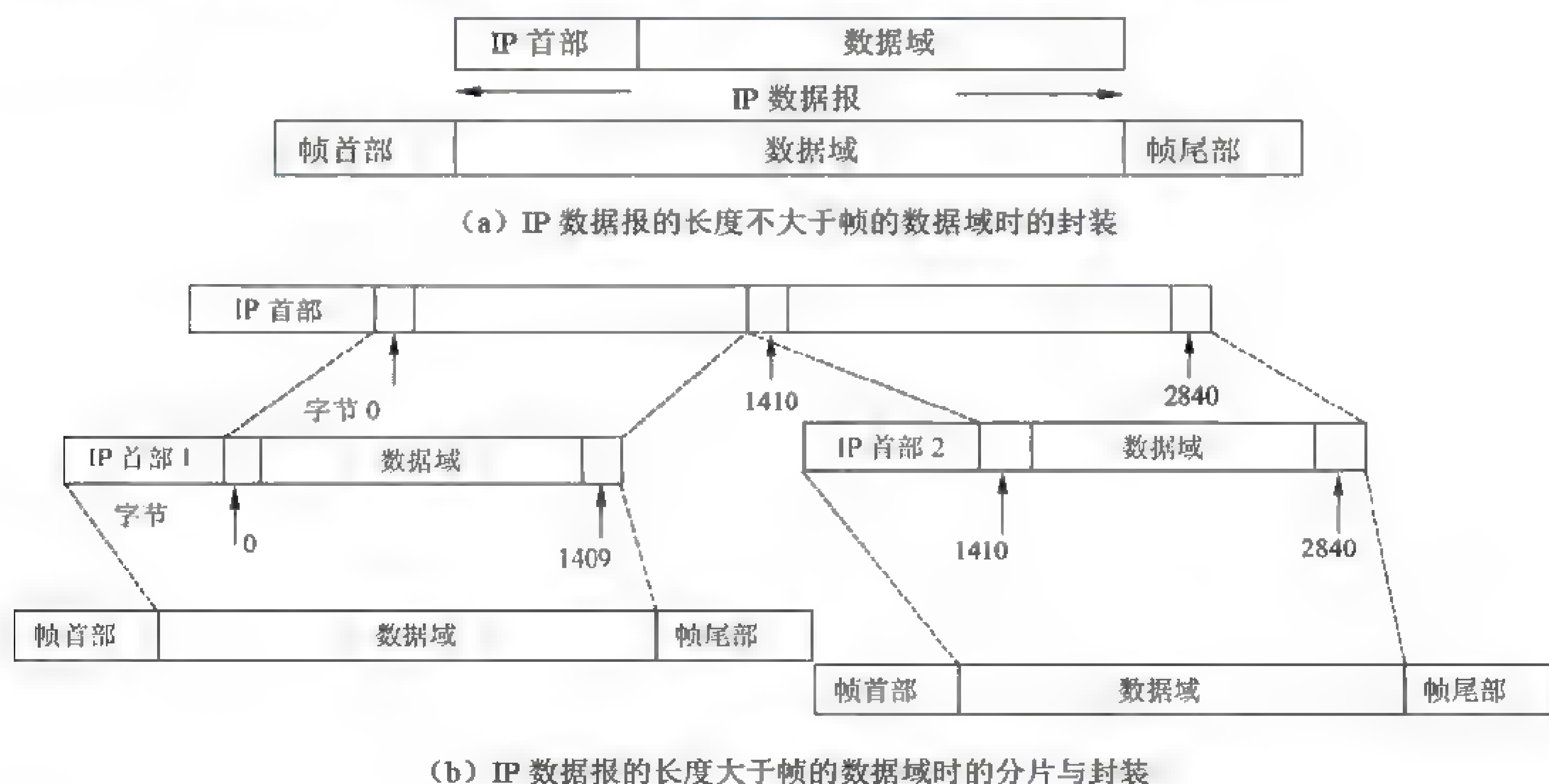


图 1-85 IP 数据报的分片与封装

1.8.1.2 Internet 路由协议

众所周知，Internet 是由多个网络互联在一起的网络，当数据包在这样一个复杂的网

络上传输时，会遇到很多“十字路口”，到底该向哪条路由上走，必须有一个类似“交警”的部件来完成这一功能。在 Internet 上这一部件就是路由器。而路由器又是依靠运行路由协议来完成其功能的。换句话说，路由器上的路由表是根据路由协议生成的。路由协议的核心就是路由算法。

由于 Internet 规模太大，所以常把它划分成许多较小的自治系统（AS）。通常把自治系统内部的路由协议称为内部网关协议，自治系统之间的协议称为外部网关协议。常见的内部网关协议有 RIP 协议和 OSPF 协议；外部网关协议有 BGP 协议。

1. 路由信息协议 RIP

RIP 是一种分布式的基于距离向量的路由选择协议。该协议定义距离就是经过的路由器的数目，距离最短的路由就是最好的路由。它允许一条路径最多只能包含 15 个路由器（限制了网络的规模）。距离的最大值为 16 时即为不可达。所以 RIP 不能在两个网络之间同时使用多条路由来进行负载均衡。

RIP 协议要求网络中的每一个路由器都要维护从它自己到其他每一个目的网络的距离记录，并依此来形成自己的路由表。且按固定时间（一般为 30s）和相邻路由器交换路由表。

RIP 协议属于应用层协议，它使用运输层的用户数据报 UDP 进行传送。RIP 协议的格式如图 1-86 所示。

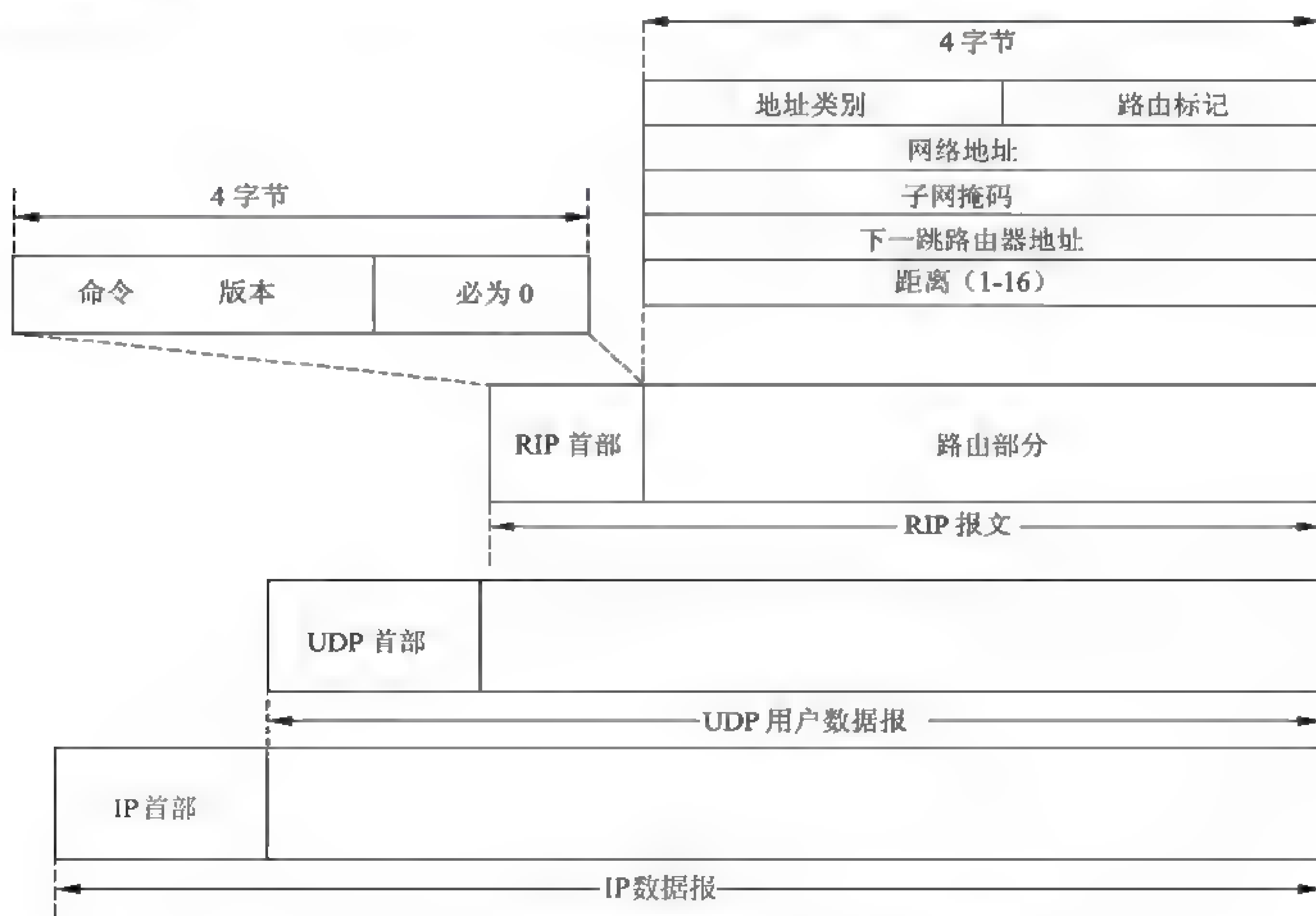


图 1-86　RIP 协议的格式及它和 UDP、IP 协议的关系

RIP 协议中的命令字段指出报文的意义。地址类别字段指出所使用的地址协议，当使用 IP 地址时，该字段的值为 2。路由标记字段应该写入自治系统号。一个 RIP 报文最大长度为 504B，这是因为一个 RIP 报文的路由部分最多可包含 25 个路由信息。当超过 504B 的最大长度时，就应该再用一个 RIP 报文来传送。

RIP 的特点是："好消息传播得快，坏消息传播得慢"。它的意思是如果路由器发现了一个更短的路由，这个消息可以很快得以传播；但如果网络出现了故障，这样的消息会传播得很慢。

2．开放最短路径优先协议（OSPF）

OSPF 协议是分布式的链路状态路由协议。链路在这里代表该路由器和哪些路由器是相邻的，即通过一个网络是可以连通的；链路状态说明了该通路的连通状态以及距离、时延、带宽等参数。在该协议中，只有当链路状态发生变化时，路由器才用洪泛法向所有路由器发送路由信息。所发送的信息是与本路由器相邻的所有路由器的链路状态。为了保存这些链路状态信息，每个路由器都建立有一个链路状态数据库，因为路由器交换信息时使用的是洪泛法，所以每个路由器都存有全网的链路状态信息，也就是说每个路由器都知道整个网络的连通情况和拓扑结构。这样每个路由器都可以根据链路状态数据库的信息来构造自己的路由表。

为了及时了解链路的状态情况，每个路由器需要定期（10s）向邻居路由器发送 Hello 分组。如果 40s 都还没有收到邻居的 Hello 信息，则认为该邻居是不连通的，应该立即修改链路状态数据库中所对应的记录，并要重新计算路由表。

除了 Hello 问候分组外，OSPF 协议还有 4 种分组：链路状态更新分组、链路状态确认分组、数据库描述分组和链路状态请求分组。通过这 4 种分组达到全网链路数据库的同步。链路状态更新分组是正常情况下，当链路状态发生变化时使用洪泛法所发送的分组；链路状态确认分组是对链路状态更新分组的确认；链路状态描述分组是当路由器启动一条新的通路时，向邻居路由器所发送的分组；链路状态请求分组是在与邻居路由器交换了数据库描述分组后，还需要其他自己缺少的路由信息时所使用的分组。

OSPF 协议格式如图 1-87 所示。

OSPF 协议使用洪泛法向网络中所有路由器发送链路状态信息为了减小洪泛范围，OSPF 协议对网络进行了区域划分。这在 OSPF 协议首部的区域标识符字段体现了出来。

3．外部网关协议（BGP）

BGP 是不同自治系统的路由器之间交换路由信息的协议。由于 Internet 的规模太大，使得自治系统之间路由选择非常困难。另外，对于自治系统之间的路由选择，要寻找最佳路由很不现实的。所以 BGP 只是尽力寻找一条能够到达目的网络且比较好的路由（不能兜圈子），而不像内部网关协议一样要寻找一条最佳路由。

每一个自治系统的管理员要选择至少一个路由器作为该自治系统的"BGP 发言人"。BGP 发言人往往就是 BGP 边界路由器，但也可以不是 BGP 边界路由器。通常，两个

BGP 发言人都是通过一个共享网络连接在一起的。

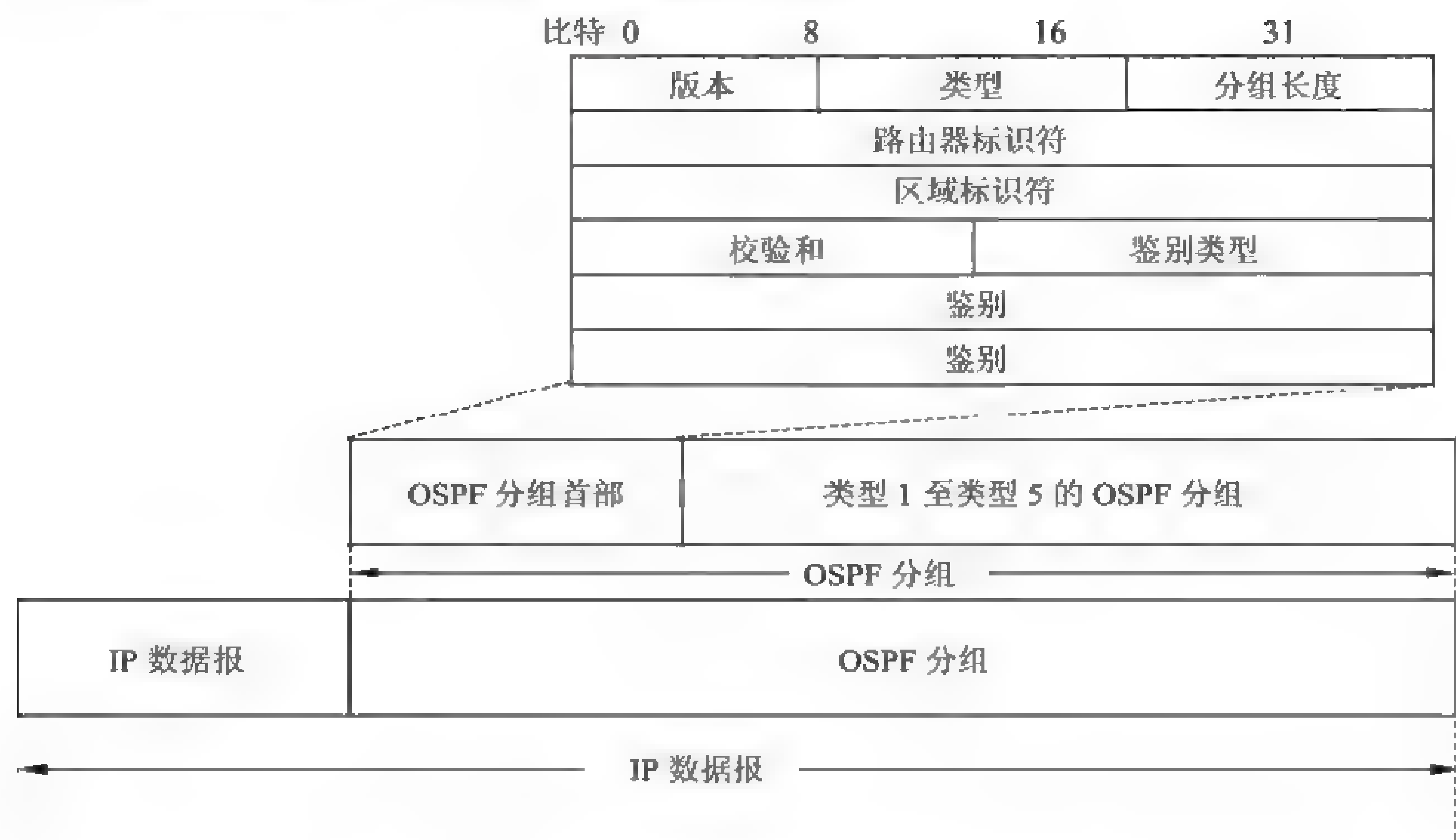


图 1-87　OSPF 协议的格式及它与 IP 协议的关系

当一个 BGP 发言人与其他自治系统中的 BGP 发言人交换路由信息时，首先要建立 TCP 连接，然后在此连接上交换 BGP 报文以建立 BGP 会话（session），利用 BGP 会话交换路由信息。

在 BGP 刚刚运行时，BGP 的邻站是交换整个的 BGP 路由表。但以后只需要在发生变化时更新有变化的部分。这样做对节省网络带宽和减少路由器的处理开销方面都有好处。

BGP 发言人互相交换网络可达性的信息后，各 BGP 发言人就可找出到达各自治系统的比较好的路由。

BGP-4 共使用 4 种报文：

- 打开（open）报文，用来与相邻的另一个 BGP 发言人建立关系。
- 更新（update）报文，用来发送某一路由的信息，以及列出要撤销的多条路由。
- 保活（keepalive）报文，用来确认打开报文和周期性地证实邻站关系。
- 通知（notificaton）报文，用来发送检测到的差错。

BGP 协议的格式及它与 TCP 和 IP 协议的关系如图 1-88 所示。

4．组播协议 PIM 与 MOSPF

IP 组播路由协议根据网络中组播组成员的分布可以分为两种基本类型：第一种被称作密集模式的组播路由协议。第二种被称为疏松模式的组播路由协议。

1）PIM（Protocol-Independent Multicast）

PIM 是一种组播传输协议，能在现存 IP 网上传输组播数据。PIM 是一种独立于路由协议的组播协议，可以工作在两种模式：密集模式（PIM-DM）和疏松模式（PIM-SM）。在 PIM 密集模式下，报文分组默认向所有端口转发，直到发生裁减和切除。在密集模式下假设所有端口上的设备都是组播成员，可能使用组播包。疏松模式与密集模式相反，只向有请求的端口发送组播数据。

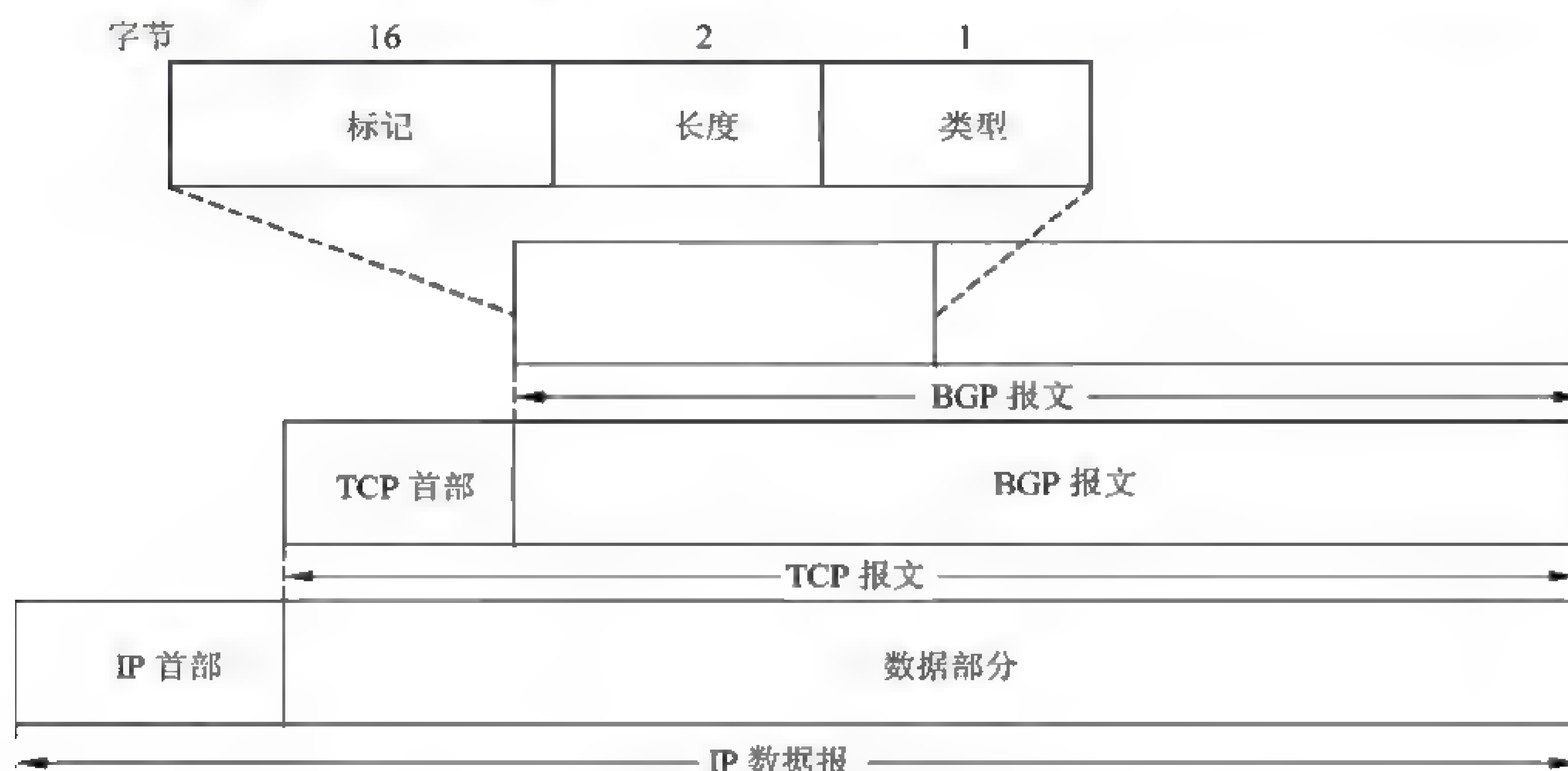


图 1-88　BGP 协议的格式及它与 TCP 和 IP 协议的关系

- PIM-SM（Protocol Independent Multicast Sparse Mode）

PIM-SM 围绕一个被称为集中点（RP）的路由器构建组播分布树。RP 是所有叶路由器都知道的点。但某个叶路由器直接相连的网络中如果有主机希望加入某 RP 所代表的组播组时，该叶路由器沿着到达 RP 的最短路径向 RP 发出加入消息，所经过的路径构成基于 RP 的单向生成树的一个新枝。一旦形成新枝，叶路由器将获得该组播组源的信息。当某个源发出的信息速率超过某个门限，则叶路由器可以切换至基于源的最短路径树上去，当然叶路由器要向 RP 方向发出剪枝消息。

PIM-SM 协议最初先为组播组构建一个组共享树。这个树由连接到集中点的发送者和接收者共同构建，就像 CBT 协议围绕着核心路由器构建的共享树一样。共享树建立以后，一个接受者（实际上是最接近这个接收者的路由器）可以选择通过最短路径树改变到发送源的连接。这个操作过程是通过向发送源发送一个 PIM 加入请求完成的。一旦从发送源到接收者的最短路径建立了，通过 RP 的外部分枝就被修剪掉了。PIM-SM 结构同时支持共享树和最短路径树这两种分布树。

- PIM-DM（Protocol-Independent Multicast-Dense Mode）

PIM-DM 协议使用了反向路径组播机制来构建分布树。PIM-DM 的运作方式是当源端送出组播信息时，它会使用先扩散再截枝的方式来建立分散树，路由器某个接收端口接收到的组播数据包被发送到所有下行接口。当末端路由器收到这个组播消息后，如果该路由器没有属于这个群组的成员，这个路由器就会向上游发出截枝的消息，而上游路由器收到这个消息时，如果该路由器也没有属于这个群组的成员，那么这个路由器又会向上游传送；反之如果该路由器有属于该群组的成员，那么这个截枝的信息就不会再往上游传送，而这个路由器就不会再把组播的资料送到这个路径上面去了。

2）MOSPF（Multicast Open Shortest Path First）

MOSPF 是为单播路由组播使用设计的，属于密集模式的组播路由协议。MOSPF 依赖于 OSPF 作为单播路由协议，在一个 OSPF/MOSPF 网络中每个路由器都维持一个最新的全网络拓扑结构图。这个“链路状态”信息被用来构建组播分布树。每个 MOSPF 路由器都通过 IGMP 协议周期性的收集组播组成员关系信息。这些信息和这些链路状态信息被发送到其路由域中的所有其他路由器。路由器将根据它们从临近路由器接收到的信息更新其内部连接状态信息。由于每个路由器都清楚整个网络的拓扑结构，所以能够独立地计算出一个最小开销扩展树，将组播发送源和组播组成员分别作为树的根和叶。这个树就是用来将组播流从发送源发送到组播组成员的路径。

1.8.1.3　地址解析协议（ARP）与反向地址解析协议（RARP）

网络中的一个机器既有逻辑地址也有物理地址。逻辑地址是为了管理方便而设置的，就像一个学生的学号，在小学有一个学号，在初中、高中和大学也各有不同的学号。而物理地址就像一个人的姓名是与生俱来的，对一个机器来说，如果不换网卡那么它永远就是网卡上那个地址。逻辑地址是网络层的协议数据单元使用的地址，物理地址是数据链路层的协议数据单元 MAC 帧使用的地址。

1．ARP 协议

在通常情况下，当我们访问一个机器的时候一定可以知道它的逻辑地址，而物理地址就不一定知道。如果不知道物理地址那么就不能把网络层的数据包封装成 MAC 帧，完不成通信。ARP 协议正是为了解决这个问题而设置的。

在每台主机上，ARP 协议都设置有一个 IP 地址和硬件地址对应关系的高速缓存。当网络层的数据报要封装成 MAC 帧时，首先在高速缓存中查看有无该数据报首部的目的地址所对应的硬件地址，若有，则将该硬件地址写入 MAC 帧的目的地址中，完成数据报的封装。若无，ARP 协议则在本局域网上广播发出一个 ARP 请求分组，格式如图 1-88 所示。在 ARP 请求分组中，发送方的 IP 地址和发送方硬件地址，以及目标 IP 地址都是应该写入已知的数据，要寻找的目标硬件地址写入全 0。当该请求分组到达每一个

机器上时，每一台机器都要拿自己的 IP 地址和请求分组中的目标 IP 地址进行比较，如果不同则不做任何动作；若相同则发送一个 ARP 相应分组给请求方。ARP 相应分组的格式同样还是和图 1-88 一样。在相应分组中发送方写明了自己的硬件地址。当这一通信过程完成时，通信双方都要对自己的 ARP 高速缓存进行修改，添加上一条记录。

ARP 协议的数据格式如图 1-89 所示。

位 0		16	31
硬件类型		协议类型	
硬件地址长度	协议长度	操作	
发送方 MAC 地址（8 位组 0～3）			
发送方 MAC 地址（8 位组 4～5）		发送方 IP 地址（8 位组 0～1）	
发送方 IP 地址（8 位组 2～3）		目标 MAC 地址（8 位组 0～1）	
目标 MAC 地址(8 位组 2～5)			
目标 IP 地址（8 位组 0～3）			

图 1-89　ARP 报文的格式

- 硬件类型：发送方想知道的硬件接口类型，以太网的值为 1。
- 协议类型：发送方提供的高层协议地址类型，IP 地址为 080616。
- 操作：ARP 请求（1），ARP 响应（2），RARP 请求（3），RARP 响应（4）。
- 协议长度：高层协议地址长度。
- 发送方 MAC 地址：发送方硬件地址。
- 目标 MAC 地址：接收方硬件地址。

2．RARP 协议

RARP 协议往往用于无盘工作站环境。因为主机没有外存，本地不能存放 IP 地址，所以需要一个 RARP 服务器来存放 IP 地址和硬件地址的对应关系。当一台主机想要上 Internet 时，它需要用自己网卡上的硬件地址到 RARP 服务器上取回自己的 IP 地址。RARP 协议的格式和 ARP 协议的格式一样。

1.8.1.4　Internet 控制报文协议（ICMP）

ICMP 协议允许路由器报告差错情况和提供有关异常情况的报告。当数据报不能正确到达目的站点，或当路由器没有足够的缓存空间，或当路由器能够向主机提供更短的路由时，ICMP 协议会及时将这些信息发送出去，就像网上的“交通警察”及时解决交通中的问题和“事故”，保证交通快速、顺畅。

ICMP 报文有 ICMP 差错报文和 ICMP 询问报文两种。

ICMP 报文格式及它与 IP 的关系如图 1-90 所示。

表 1-8 给出了几种常用的 ICMP 报文类型。

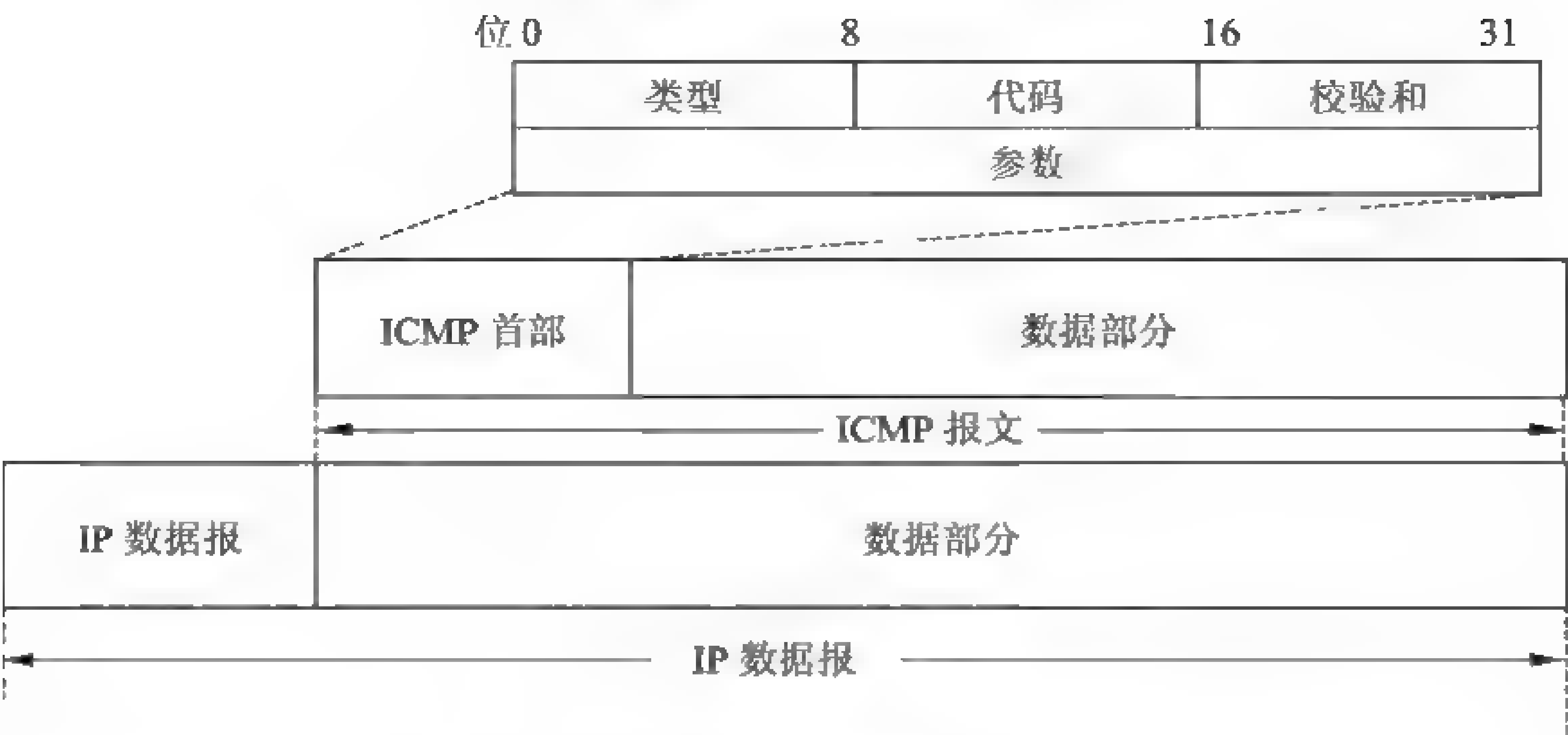


图 1-90　ICMP 报文格式及它与 IP 的关系

表 1-8　几种 ICMP 报文及功能

ICMP 报文类型	类型的值	ICMP 报文的类型	功　能
差错报告报文	3	终点不可达	当路由器不能把数据报转交给目的站时，就向源站发送终点不可达报文
	4	源站抑制	当路由器由于拥塞而丢弃数据报时，就向源站发送源站抑制报文，使源站放慢数据报的发送速度
	5	改变路由	当路由器发现主机可以把数据报发送给另外一个路由器，使数据报沿着更短更好的路由被转发
	11	时间超时	当路由器收到一个 IP 数据报时，发现它的生存时间为 0，或主机在预订的时间内无法完成数据报的重装，则向源站发送时间超时报文
	12	参数问题	当路由器或目的站发现收到的数据报首部字段中有不正确的字段时，就向源站点发送参数问题报文
询问报文	8 或 10	回送请求或回答	当需要测试某一目的站点是否可达时，就发送一个 ICMP 回送请求报文，然后目的站点会向发送站回送一个 ICMP 回答报文
	13 或 14	时间戳请求或回答	当需每个路由器或主机给出当前的日期和时间时，就发送时间戳请求报文，然后被请求方会回送一个时间戳回答报文，告知自己当前的日期和时间。这样可以用来测试通信延迟

1.8.1.5 IPv6 协议

1. IPv6 协议的特点

- 更大的地址空间。IPv6 将地址从 IPv4 的 32bit 增大到了 128bit。
- 扩展的地址层次结构。
- 灵活的首部格式。
- 改进的选项。
- 增强安全性。
- 对 QoS 支持。

2. IPv6 地址

IPv6 地址格式如图 1-91 所示。

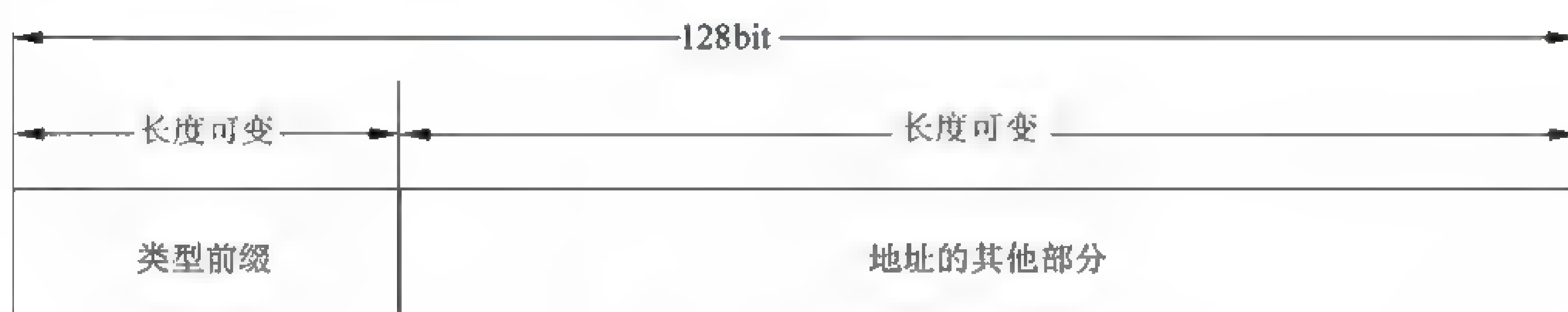


图 1-91 IPv6 地址格式

IPv6 将 128bit 地址空间分为两大部分。第一部分是可变长度的类型前缀，它定义了地址的目的。第二部分是地址的其余部分，其长度也是可变的。

每个 16bit 的值用十六进制值表示，各值之间用冒号分隔。

IPv6 数据报的目的地址可以是以下三种基本类型地址之一：

- 单播（unicast）：单播就是传统的点对点通信。
- 多播（multicast）：多播是一点对多点的通信。
- 任播（anycast）：这是 IPv6 增加的一种类型。任播的目的站是一组计算机，但数据报在交付时只交付给其中的一个，通常是距离最近的一个。

前缀为 0000 0000 是保留一小部分地址与 IPv4 兼容的，这是因为必须要考虑到在比较长的时期 IPv4 和 IPv6 将会同时存在，而有的节点不支持 IPv6。

IPv6 扩展了地址的分级概念，使用以下三个等级：

- 第一级（顶级），指明全球都知道的公共拓扑。
- 第二级（地点级），指明单个的地点。
- 第三级，指明单个的网络接口。

3. IPv6 包格式

IPv6 数据包格式如图 1-92 所示。



图 1-92　IPv6 数据包格式

（1）对 IPv6 基本报头各域的说明如下。

- 版本（version）：4bit，它指明了协议的版本，对 IPv6 该字段总是 6。
- 通信量类（Traffic Class）：8bit，这是为了区分不同的 IPv6 数据报的类别或优先级。
- 流标号（Flow Label）：20bit，用于源节点标识 IPv6 路由器需要特殊处理的包序列。
- 载荷长度（Payload Length）：16bit，它指明 IPv6 数据报除基本首部以外的字节数（所有扩展首部都算在有效载荷之内），其最大值是 64KB。
- 下一个报头（Next Head）：8bit。它相当于 IPv4 的协议字段或可选字段。
- 跳数限制（Hop Limit）：8bit。源站在数据报发出时即设定跳数限制。路由器在转发数据报时将跳数限制字段中的值减 1。当跳数限制的值为 0 时，就要将此数据报丢弃。
- 源地址（Source Address）：128bit，指明生成数据包的主机的 IPv6 地址。
- 目的地址（Destination Address）：128bit，指明数据包的最终要到达的目的主机的 IPv6 地址。

（2）IPv6 的扩展首部。

IPv6 将原来 IPv4 首部中选项的功能都放在扩展首部中，并将扩展首部留给路径两

端的源站和目的站的主机来处理。数据报途中经过的路由器都不处理这些扩展首部（只有一个首部例外，即逐跳选项扩展首部）。这样就大大提高了路由器的处理效率。

在[RFC 2460]中定义了6种扩展首部。

- 逐跳选项：此扩展头必须紧跟在IPv6基本报头之后，它包含所经路径上的每一个节点都必须检查的选项数据。由于它需要在每个中间路由器都进行处理，所以只有在绝对必要的时候才出现。
- 路由选择：此扩展头指明数据包在到达目的地途中将经过地各节点的地址列表。
- 分片：当IPv6源地址发送的数据包比到达目的地址所经过的路径上的最小MTU还要大时，这个数据包就要被分成几段分别发送，这时就要用到分片头。
- 鉴别：鉴别头的功能是实现了数据的完整性和对数据来源的认证。
- 封装安全有效载荷：封装安全有效载荷头提供数据加密功能，实现端到端的加密，提供无连接的完整性和防重发服务。封装安全载荷头可以单独使用，也可以在使用隧道模式时嵌套使用。
- 目的站选项：目的站选项头中携带仅需要有最终目的节点检验的可选信息。它要在IPv6目的地址域所列的第一个目的主机上处理，也要在路由头所列的后续目的主机上处理。

4．IPv6地址自动配置

IPv6中地址自动配置有两种方式：有状态地址自动配置和无状态自动配置，当站点并不是特别关心主机所使用的精确地址时，只要它们是唯一的，并且是可路由的，就能使用无状态方式；当站点严格控制地址分配时，就使用有状态方式。

1）有状态自动配置

在这种模式下，主机可以从服务器获得接口地址，也可以从服务器上获得配置信息和参数。服务器中维护着一个数据库，其中记录着主机和地址分配的列表。比较常用的是DHCPv6（Dynamic Host Configuration Protocol for IPv6）协议，即支持IPv6的动态主机配置协议。它允许DHCPv6服务器把诸如IPv6网络地址等信息传给IPv6节点。DHCPv6服务器与客户端使用UDP来交换DHCPv6报文。服务器和中继代理使用UDP端口547来监听DHCPv6报文；客户端使用UDP端口546来监听报文。

2）无状态地址自动配置

无状态自动配置要求本地链路支持组播。而且网络接口能够发送和接收组播包。采用这种方式可以为任意主机配置一个IPv6地址，这个地址内嵌一个以太网地址，由于以太网地址全球唯一，因此获得的IPv6地址也是唯一的。

具体过程如下：

首先，进行自动配置的节点必须确定自己的链路本地地址。

然后，必须验证该链路本地地址在链路上的唯一性。

最后，节点必须确定需要配置的信息。该信息可能是节点的IP地址，或者是其他配

置信息，或者两者皆有。具体地说，在无状态自动配置过程中，主机首先通过将它的网卡 MAC 地址附加在链路本地地址前缀 1111111010 之后，产生一个链路本地单播地址（IEEE 已经将网卡 MAC 地址由 48 位改为了 64 位。如果主机采用的网卡的 MAC 地址依然是 48 位，那么 IPv6 网卡驱动程序会根据 IEEE 的一个公式将 48 位 MAC 地址转换为 64 位 MAC 地址）。接着主机向该地址发出一个邻居发现请求（neighbor discovery request），以验证地址的唯一性。如果请求没有得到响应，则表明主机自我配置的链路本地单播地址是唯一的。否则，主机将使用一个随机产生的接口 ID 组成一个新的链路本地单播地址。然后，以该地址为源地址，主机向本地链路中所有路由器多点传送一个路由器请求（router solicitation）来请求配置信息，路由器以一个包含一个可聚集全球单播地址前缀和其他相关配置信息的路由器宣告（router advertisement）作为响应。主机用它从路由器得到的全球地址前缀加上自己的接口 ID，自动配置全球地址，然后就可以与 Internet 中的其他主机通信了。

如果本地网络孤立于其他网络，则节点必须寻找配置服务器来完成其配置；否则，节点必须侦听路由器宣告报文。这些报文周期性地发往所有主机的组播地址，以指明诸如网络地址和子网地址等配置信息。节点可以等待路由器宣告，也可以通过发送组播请求给所有路由器的组播地址来请求路由器发送宣告。一旦收到路由器的响应，节点就可以使用响应的信息来完成自动配置。

5. 邻节点发现过程

邻居发现协议使用一系列的 IPv6 控制信息报文来实现相邻节点的信息交互管理，并在一个子网中保持网络层地址和链路层地址之间的映射。邻居发现协议中定义了 5 种类型的信息：路由器宣告、路由器请求、路由重定向、邻居请求和邻居宣告。

- 路由器发现：即帮助主机来识别本地路由器。
- 前缀发现：节点使用此机制来确定指明链路本地地址的地址前缀以及必须发送给路由器转发的地址前缀。
- 参数发现：帮助节点确定诸如本地链路 MTU 之类的信息。
- 地址自动配置：用于 IPv6 节点自动配置。
- 地址解析：替代了 ARP 和 RARP，帮助节点从目的 IP 地址中确定本地节点（即邻居）的链路层地址。
- 下一跳确定：可用于确定包的下一个目的地，即可确定包的目的地是否在本地链路上。如果在本地链路，下一跳就是目的地；否则，包需要选路，下一跳就是路由器，邻居发现可用于确定应使用的路由器。
- 邻居不可达检测：帮助节点确定邻居（目的节点或路由器）是否可达。
- 重复地址检测：帮助节点确定它想使用的地址在本地链路上是否已被占用。
- 重定向：有时节点选择的转发路由器对于待转发的包而言并非最佳。这种情况下，该转发路由器可以对节点进行重定向，使它将包发送给更佳的路由器。

1.8.1.6 IPv4 向 IPv6 的过渡

在 IPv4 向 IPv6 过渡时，只能采用逐步演进的办法，整个过渡需要一个比较漫长的过程。在过渡期间，由于 IPv4 和 IPv6 在很长一段时期内会共存，因此很有必要解决 IPv4 和 IPv6 之间相互通信的问题。

目前 IPv4/IPv6 过渡技术主要有三种方案：隧道技术、双协议栈技术和地址协议转换（NAT-PT）。

1．双协议栈

双协议栈（dual stack）是指在完全过渡到 IPv6 之前，使一部分主机（或路由器）装有 IPv4 和 IPv6 两个协议栈，如图 1-93 所示。

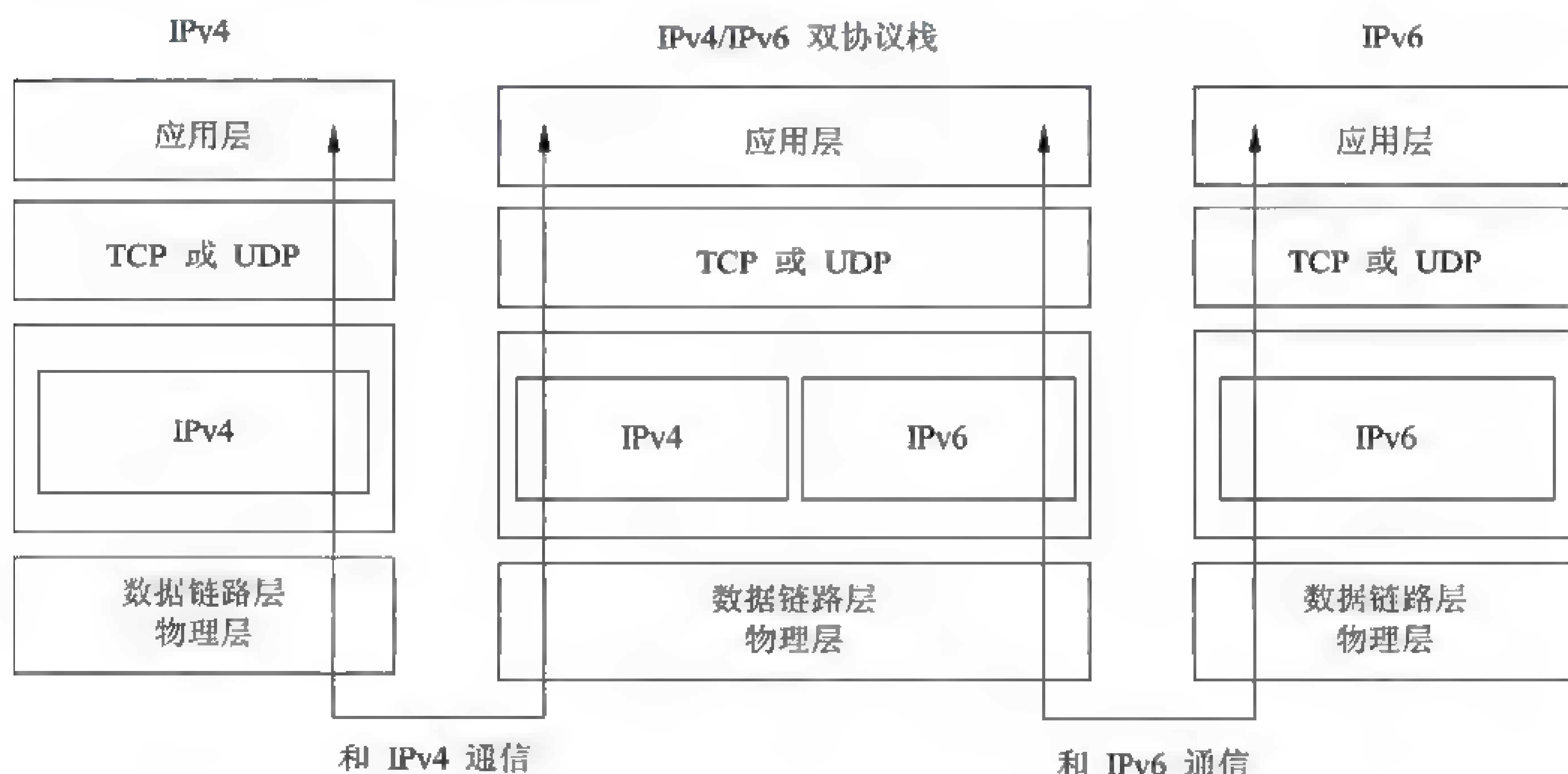


图 1-93 使用双协议栈从 IPv4 到 IPv6 过渡

对于主机而言，双协议栈是指其可以根据需要来对上层协议所产生的数据进行 IPv4 封装或者 IPv6 封装。

对于路由器而言，分别支持独立的 IPv6 和 IPv4 路由协议，IPv4 和 IPv6 路由信息按照各自的路由协议进行计算，维护两张不同的路由表。

2．隧道技术

隧道策略是 IPv4/IPv6 过渡中经常使用到的一种机制（如图 1-94 所示）。隧道技术的工作机理就在 IPv6 网络与 IPv4 网络间的隧道入口处，路由器将 IPv6 的数据分组封装入 IPv4 中，IPv4 分组的源地址和目的地址分别是隧道入口和出口的 IPv4 地址。在隧道的出口处再将 IPv6 分组取出转发给目的节点。隧道技术巧妙地利用了现有的 IPv4 网络，为分离的 IPv6 子网（或主机）提供了有效的通信手段。隧道技术能够充分利用现有的网

络投资，因此在过渡初期是一种简单方便的选择。但是，在隧道的入口处会出现负载协议数据包的拆分，在隧道出口处会出现负载协议数据包的重组。这就增加了隧道出入口的实现复杂度，不利于大规模的应用。并且隧道技术只能够实现 IPv6 与 IPv6 之间的通信，不能够解决 IPv6 和 IPv4 之间的互通问题。

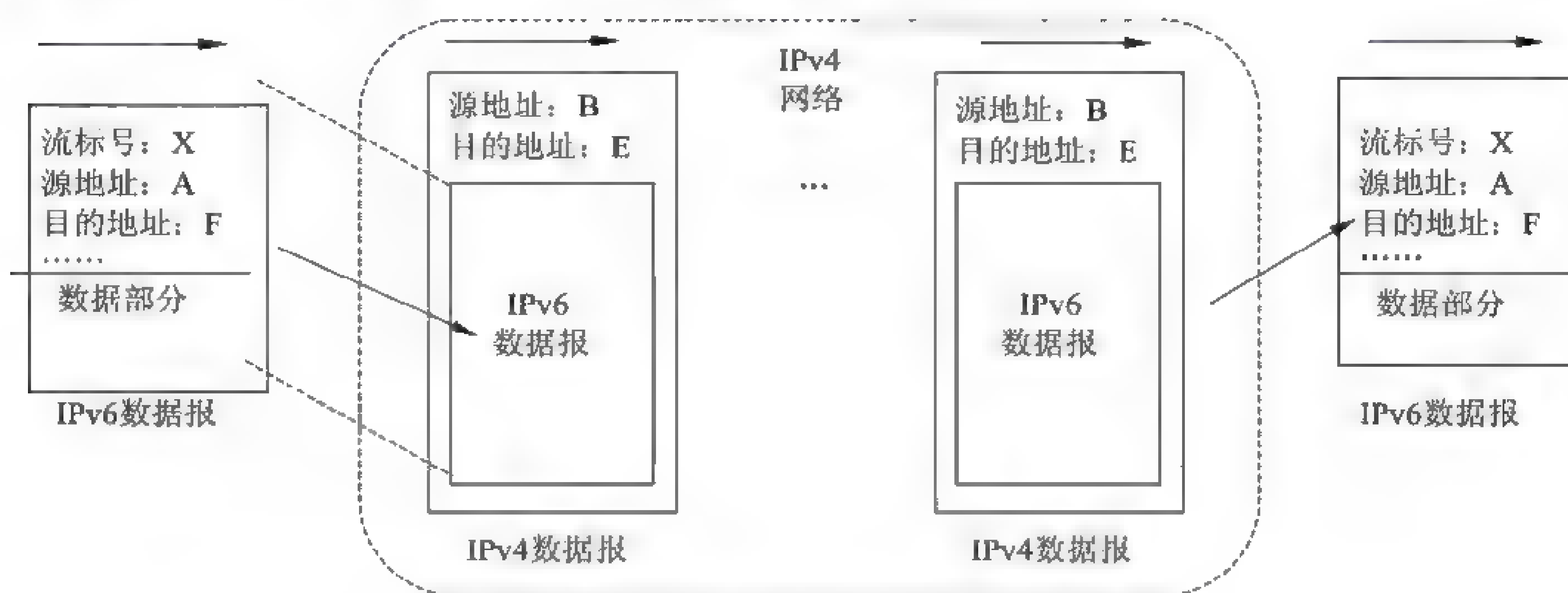


图 1-94　使用隧道技术从 IPv4 到 IPv6 过渡

3. NAT-PT

NAT-PT（网络地址转换-协议转换）包括两个组成部分：网络地址转换协议和协议转换。其中地址转换是指通过使用 NAT 网关将一种 IP 网络的地址转换为另一种 IP 网络的地址，它允许内部网络使用一组在公网中从不使用的保留地址。在使用这项技术时可以将 IPv6 网视为一个独立而封闭的局域网，它需要使用一个地址翻译器进行地址翻译。

协议转换是指根据 IPv6 和 IPv4 之间的差异对数据包的首部做相应的修改以符合对方网络的格式要求，并且由于网络层协议的改变要对上层的 TCP，UDP，ICMP 等数据包做相应的修改。将网络地址转换机制与协议转换机制相结合而产生的 NAT-PT 可以通过对协议、地址的转换实现 IPv6 和 IPv4 之间的相互通信。

NAT-PT 的优点是所有的地址转换和协议转换都在 NAT-PT 服务器上完成，而子网内部的主机不需要做任何改动，就可以实现两个不同子网之间的相互访问。同样由于所有的 IP 数据包都要在 NAT-PT 服务器上做数据包的修改，使得它们常常会破坏端到端服务（如端到端的 IP 安全），这一点和 IPv4 中的 NAT 类似。同时，翻译器还会造成网络潜在的单故障点。同时 NAT-PT 实现起来比较复杂，牵涉到如何简单快速地实现网络地址和端口分配及数据包的快速修改。由于有大量的数据包在 NAT-PT 服务器上处理，因此 NAT-PT 服务器的处理能力成为两个网络之间通信的瓶颈。

1.8.1.7　移动 IP 协议

1. 移动 IP 技术的功能实体

移动 IP 定义了三个功能实体：移动节点、归属代理和外区代理。

- 移动节点（Mobile Node，MN）：当节点从一条链路切换到另一条链路上时仍能保持所有正在进行通信的移动主机。它有两个 IP 地址：一个是归属地址（home address），用来标识 TCP 连接的永久地址；另一个是转交地址（Care of Address，CoA），是当移动节点漫游到其他子网时所获得的供 IP 包选路使用的临时地址。转交地址可以由外地代理提供，称为代理转交地址（agent CoA），也可以由外地网络的 DHCP 服务器分配，称为配置转交地址（Collocated CoA，CCoA）。两种地址的不同在于后者是一个“真实”的转交地址，而前者是代理的某个接口地址。
- 归属代理（Home Agent，HA）：移动节点本地网络上的路由器。它有一个端口与移动节点家乡链路相连，同时保存移动节点的位置信息。当移动节点离开归属网络时，它能够将发往移动节点的数据包传给移动节点。归属代理广播对移动节点家乡地址的可达性，从而吸引那些送往移动节点归属地址的 IP 数据包，接着它将解析送往移动节点的归属地址的数据包，并将它们通过隧道技术传送到移动节点的转交地址上。
- 外区代理（Foreign Agent，FA）：移动节点当前连接到的外地网络上的路由器。其作用是为移动节点提供路由服务，并且对经归属代理封装后发给移动节点的数据包进行解封装，然后转发给移动节点。

2．移动 IP 技术的工作机制

移动 IP 的工作过程如下：

① 归属代理和外区代理周期性发送组播或广播报文，以此向它们所在的网络中的节点通告它们的存在。

② 移动节点收到广播报文后，检查报文的内容来判断它所连接的是归属网络还是外地网络。当连在归属网络上时，采用传统的 IP 通信方式而不使用移动 IP 的功能。如果是从外地网络重新返回的，则向本地代理发出取消注册的功能消息，声明自己回到了本地网。

③ 当移动节点移动到外地网络时，它可以从当前网络的外区代理发出的代理广播消息中获得转交地址，或者通过 DHCP 服务器配置获得。

④ 移动节点通过外区代理向归属代理注册转交地址，注册可以通过移动 IP 中定义注册消息来完成。

⑤ 归属代理对移动节点的注册请求进行鉴权、认证。归属代理通过发送注册成功消息到移动 IP 的转交地址来标志注册的完成。

⑥ 注册完毕后，所有发给移动主机的数据包被本地代理截获，经本地代理封装后通过隧道发到外地网络的外区代理 FA（代理转交地址）或移动主机自身（配置转交地址）。在采用代理转交地址的情况下，外地代理再把数据包转发给移动主机。此时，数据包在不同子网间传送成功。

⑦ 移动节点发往与它通信的主机的数据会直接经过外地代理转发到相应主机。这就形成了一个“三角路由”。

3．移动 IP 技术中的几项关键技术

移动 IP 与传统 IP 协议相比，主要使用了下列几个关键技术。

1）隧道技术

隧道技术是归属代理把原先发往移动节点的数据包，封装在发向转交地址的数据包中，并在外区代理中解包，然后传向移动节点的当前位置。通过该技术，避免了从归属链路到外部链路上所有路由器的路由信息改动。当其他节点向移动节点发送数据包时，归属代理截获该数据包，使用隧道技术把数据包向外区代理发送。这是通过 IP in IP 封装来实现的，如图 1-95 所示。

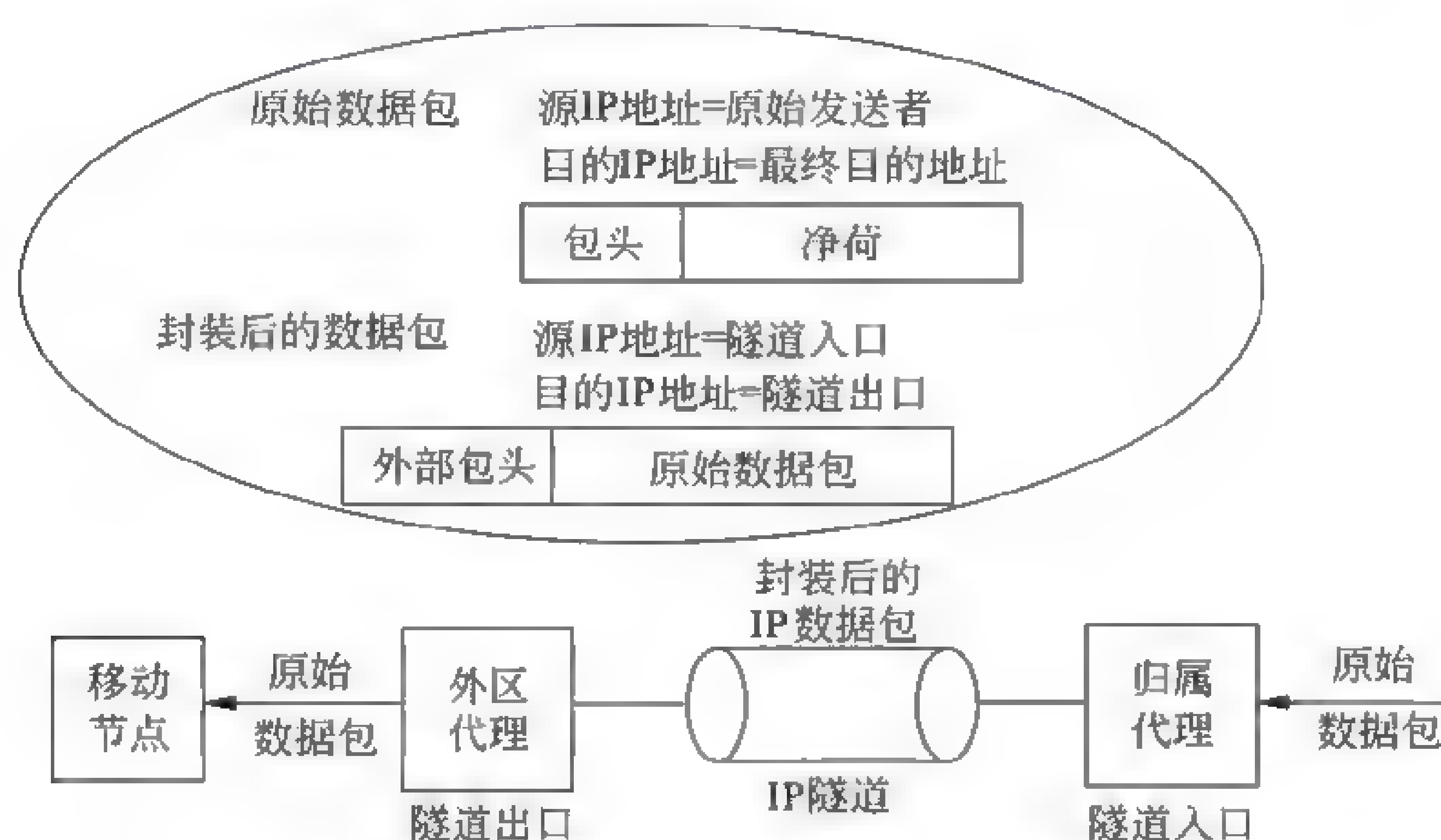


图 1-95　隧道技术

2）代理搜索

代理搜索通过两种消息来实现：代理请求消息和代理广播消息。代理搜索基于 ICMP 协议之上。代理请求消息是在移动节点没有耐心等待代理广播消息时由移动节点发送的。它的目的是为了让链路上的所有代理发送一个广播代理消息，该消息比较简单。代理广播消息用来实现代理搜索的所有功能。

3）注册

注册发生在代理搜索之后，是移动主机把搜索获得的转交地址及时通知到隧道入口（归属代理）的方法。它在以下三种情况下都会发生：① 当移动主机切换网络时；② 当移动主机发现所连接的外地代理重启时；③ 当移动主机的现有注册到期时。

注册过程是移动主机和归属代理间一次注册请求和注册应答的交互。注册的实现有两种方式一是移动主机用外地代理转交地址注册，如图 1-96 所示。

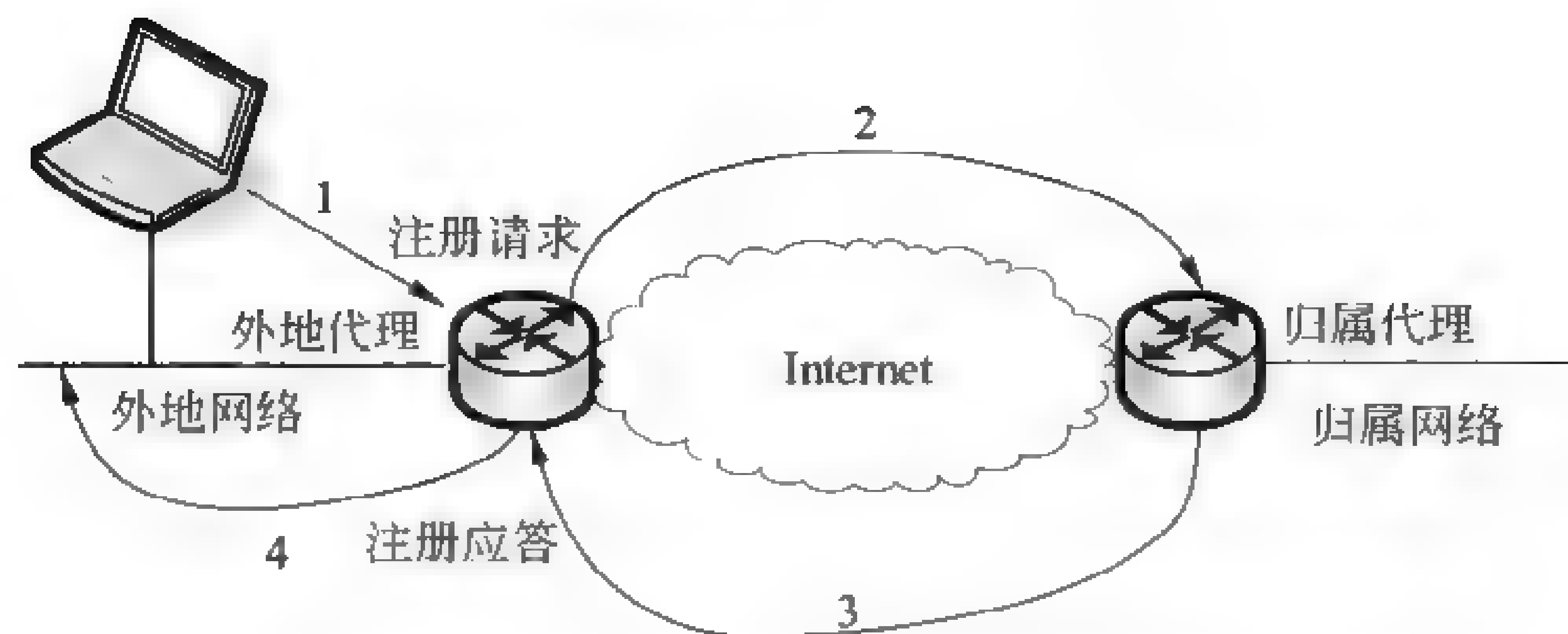


图 1-96 移动主机使用外地代理转交地址的注册过程

此时注册的实现过程为移动主机根据搜索所得消息产生注册请求信息，并发送给外地代理，等待注册应答→外地代理先检查收到的请求消息，没问题就记下发回应答所要的信息，再将请求中继给归属代理→归属代理检查该请求，若请求无效，则发送表注册失败的应答；若有效，则更新本地地址、转交地址对应表中的绑定表项，做对应于请求的操作，最后向外地代理发送表注册成功的应答→外地代理对注册应答进行有效性检查。若应答无效就产生一个含 Code 域的应答送给移动主机；应答有效就更新来访移动主机的列表，将应答中继给移动主机→移动主机先检查应答的有效性，若有效，再检查注册被代理接受与否的 Code 域，若被拒绝则修正错误并尝试重新注册，若被接受就调整路由表以适应当前网络，停止重发注册请求。

二是移动主机用配置转交地址注册，如图 1-97 所示。

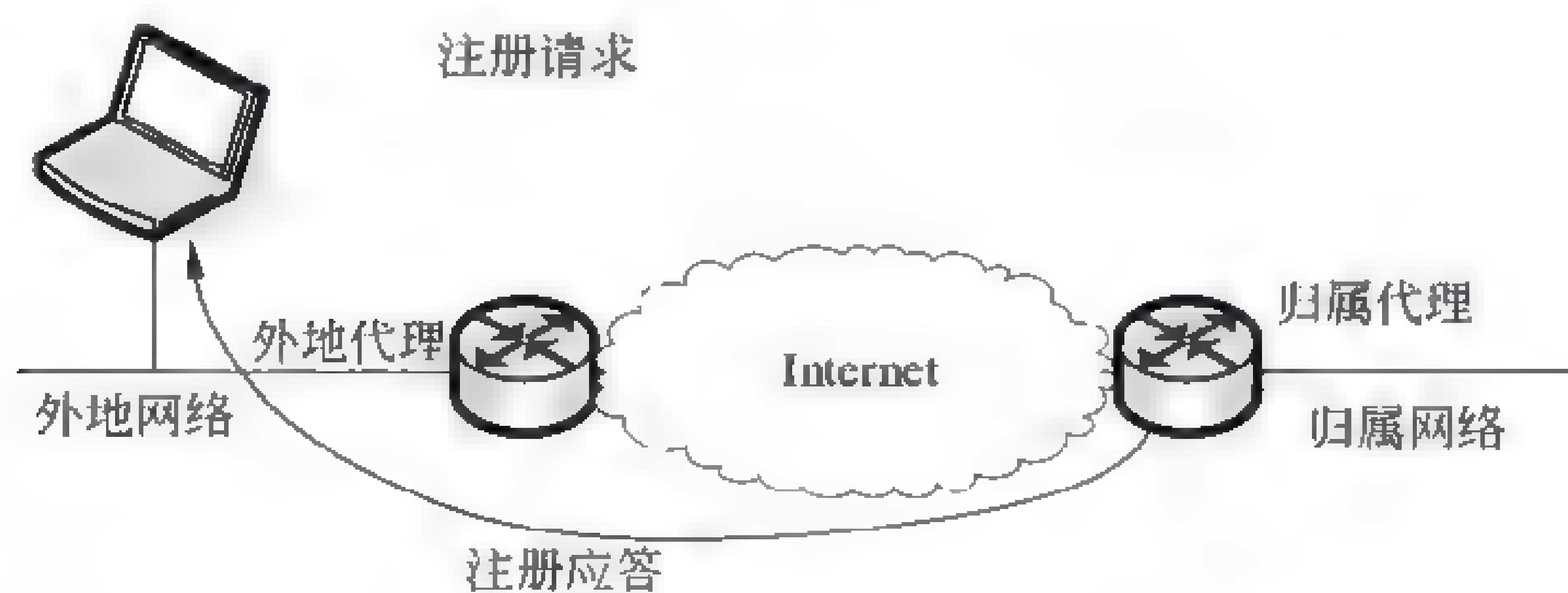


图 1-97 移动主机使用配置转交地址的注册过程

此时注册过程相对简单，不需要通过外地代理，具体过程为移动主机向归属代理发送注册请求消息→归属代理处理注册请求并发回注册应答→移动节点处理注册应答。

1.8.1.8 QoS 支持

1. QoS 概述

服务质量（Quality of Service，QoS）是服务性能的总效果，此效果决定了一个用户对服务的满意程度。因此在最简单的意义上，有服务质量的服务就是能够满足用户的应

用需求的服务。

在 Internet 上为用户提供高质量的 QoS 必须解决以下几个问题。

- QoS 的分类与定义：对 QoS 进行分类和定义的目的是使网络可以根据不同类型的 QoS 进行管理和分配资源。例如，给实时服务分配较大的带宽和较高的 CPU 处理时间等；另一方面，对 QoS 进行分类定义也方便用户根据不同的应用提出 QoS 需求。
- 准入控制和协商：根据网络中资源的使用情况，允许用户进入网络进行多媒体信息传输协商其 QoS。
- 资源预约：为了给用户提供满意的 QoS，必须对端系统、路由器以及传输带宽等相应的资源进行预约，以确保这些资源不被其他应用所抢用。
- 资源调度与管理：资源进行预约之后，是否能得到这些资源，还依赖于相应的资源调度与管理系统。

2．QoS 的若干性能指标

服务质量可用若干基本的性能指标来描述，包括可用性、差错率、响应时间、吞吐量、分组丢失率、连接建立时间、故障检测和改正时间等。

3．由 QoS 控制来实现 QoS 保证的策略

IP 网络如何提供服务质量 QoS 支持这一问题已经成为业界关注的焦点。对于由 QoS 控制来实现 QoS 保证，国际上不同组织和团体提出了不同的控制机制和策略，比较著名的有以下一些：

- ISO/OSI 提出了基于 ODP 分布式环境的 QoS 控制，至今仍只停留在给出了用户层的 QoS 参数说明和集成接口阶段，具体实现 QoS 的控制策略并未提出。
- ATM 论坛提出了 QoS 控制的策略和实现，ATM 控制是“连接预定（connection and reservation）”型，它的核心内容是在服务建立之前，通过接纳控制和资源预留来提供服务的 QoS 保证，而在服务交互的过程中，用户进程和网络要严格按照约定的 QoS 实现服务 QoS 保证。
- IETF 组织也已经提出了多种服务模型和机制来满足对 QoS 的需求，其中比较典型的有：RFC2115，RFC2117 以及 1998 年、1999 年提出的 RFC26xx 系列中的综合业务模型、差分业务模型、多协议标签 MPLS 技术、流量工程和 QoS 路由等，均用于解决 Internet 的 QoS 控制和管理。

4．主要的 QoS 技术

当前主要的 QoS 技术有集成服务（Integrated Services，IntServ）/资源预留协议（RSVP）、区分业务（Differentiated Services，DiffServ）、多协议标记交换（Multi-Protocol Label Switching，MPLS）、流量工程（Traffic Engineering）、QoS 路由（QoS Routing，QoSR）等。

1）集成服务（IntServ）

IntServ 其基本思想是一个应用要想获得某种服务质量，必须在向网络传送流量之前请求网络为其预留所需资源。因此从某种意义上来说，IntServ 实际上是提供了一种类似于电路级的服务质量。

在结构层次上，IntServ 服务模型主要由以下 4 部分构成：

- 资源预留协议 RSVP，它是 IntServ 的信令协议，负责逐点（hop-by-hop）地建立或者拆除每个流的资源预留软状态（soft state），即建立或拆除数据传输路径。
- 接纳控制，用来决定是否同意对某一资源的请求，其根据是链路和网络节点的资源使用情况以及 QoS 请求的具体要求。
- 分类器，用来将进入路由器的分组进行分类，并根据分类的结果将不同类别的分组分别放入不同类别的队列。IntServ 常用的分类器是多域分类器，当路由器接收到数据包时，它根据数据包头部的多个域（如源 IP 地址、目的 IP 地址、源端口号、目的端口号、传输协议），将数据包放入相应的队列中。
- 调度器（packet scheduler），根据不同的策略对各个队列中的数据包进行调度转发。

使用 RSVP 信令建立数据发送路径以及为业务流预留资源的过程可分为下面几步。

① 数据发送的源端确定发送数据流所需的带宽、延迟和延迟抖动等指标（即 TSPEC 参数），并将其包含在 PATH 控制消息中发送给接收端。

② 各 RSVP 路由器解释 PATH 消息，保存上一中继的 IP 地址，将自己的 IP 地址作为前一中继段地址，并沿应用程序数据使用的路由发送更新后的消息。

③ 接收端收到 PATH 消息后，它沿着与 PATH 消息中获取的源路径相反的方向向上一中继段路由器发送一个 RESV 消息。该 RESV 消息包含为数据流进行资源预留所需要描述的流量和性能期望等 QoS 信息。

④ RSVP 路由器接收到 RESV 消息时，它通过接纳控制来确定是否可以满足这些 RESV 请求。如果可以，就合并收到的预留请求，进行带宽和缓冲区空间的预留，并且存储一些与数据流相关的特定信息，并将 RESV 消息转发给上一中继段路由器请求预留。如果不能，就拒绝预留，同时返给接收端一个错误信息。

⑤ 如果源端收到 RESV 消息，则表明数据流的资源预留已经成功，可开始向接收端发送数据。

⑥ 当数据流发送完毕，路由器可以释放先前设置的预留资源。

IntServ 模型的优点如下：

- 提供绝对保证的 QoS，因为 RSVP 在从源端到目地端的每个路由器上运行，能监视每个数据流，以防资源浪费。
- 在源端与目的地之间，RSVP 可以用现有的路由协议决定数据流的通路，RSVP 使用 IP 包承载，通过周期性重传路径和 RESV 消息，能对网络拓扑的变化做出反应。

- 可支持多播流，RSVP 协议能让路径消息识别多播流的所有端点，并将路径消息发送给它们，还能把来自每个接收端的 RESV 消息合并到一个网络请求点上，让一个多播流能在分开的连接上发送。

IntServ 模型的缺点如下：

- 状态信息的数量与流的数目成正比。因此在大型网络中，按每个流进行资源预留会产生很大的开销。
- IntServ 体系结构复杂。若要得到有保证的服务，所有的路由器都必须装有 RSVP、接纳控制、分类器和调度器。
- 综合服务 IntServ 所定义的服务质量等级数量太少，不够灵活。

2）区分服务（DiffServ）

DiffServ 模型的基本思想是根据预先确定的规则对数据流进行分类，将具有相同 QoS 需求的不同业务的数据流聚集成一个数据流集合进行统一处理，以便将多种应用数据流综合为有限的几种数据流等级，不同的数据流集合获得不同的优先级处理。DiffServ 模型是为克服 IntServ 模型的扩展性问题，从 IntServ 模型发展而来的一种相对简单的、较粗糙的提供区别服务等级（Class of Service，CoS）的模型。它采用了 IETF 的基于 RSVP 的服务分类标准，但抛弃了分组流沿路节点上的资源预留。

DiffServ 将 IPv4 协议中原有的服务类型字段和 IPv6 的通信量类字段定义为区分服务字段 DS。该字节中的前 6 个比特称为区分服务编码点，用于 QoS 的特殊定义，包括“等级”和“丢弃优先级”。另外，DiffServ 将整个网络分成若干个 DS 域，一个 DiffServ 域由一系列支持 DiffServ 机制的节点构成。在 DiffServ 域中，主要的成员有边缘路由器、核心路由器和资源控制器。

当数据流进入 DiffServ 网络时，边缘路由器通过标识该字段，将 IP 包分为不同的服务类别，而网络中的其他路由器在收到该 IP 包时，则根据该字段所标识的服务类别将其放入不同的队列，并由作用于输出队列的流量管理机制，按事先设定的带宽、缓冲处理控制每个队列，即给予不同的每一跳行为（PerHopBehaivor，PHB）。

总之，DiffServ 根据每个 IP 包头中的 DS 字段，可以将其归类到与其具有相同 QoS 需求的一个数据集合中去，这样，众多的数据流被归类成了几个为数不多的具有相同 QoS 需求的数据集合进行传送，然后根据与每个数据集合相对应的处理方式对这些数据集合进行处理。这种模型简化了数据流的处理过程，减少了路由器中信息存储的负担；同时也免去了 IntServ/RSVP 模型中在网络内部建立路由通道的操作，从而减少了主机之间简短对话的负荷，提高了网络的响应性能。

具体工作流程如下：

① 首先 DiffServ 域的边缘路由器对来自用户或其他网络的非 DiffServ 的业务流进行分类，为每个 IP 包填入新的 DSCP 字段；同时，建立起并开始应用与每一个业务相对应的服务水平协定（SLA）和 PHB。而对来自用户或其他网络的 DiffServ 业务流，则依据

IP 包中的 DSCP 字段选择特定的 PHB。

② 然后开始业务转发，边缘路由器的策略单元将根据 SLA 对收到的业务流进行测量，监视用户是否遵守 SLA，并将测量结果输入业务流策略单元，对业务流进行整形、丢弃、标记（DSCP 的改写）等工作。这一过程称为业务量调整（traffic conditioning）或业务量策略（traffic policing）。

③ 边缘路由器对 DSCP 字段进行检查，依据 DSCP 为业务流选择特定的 PHB，根据 PHB 所指定的排队策略，将属于不同业务类别的业务流导入不同的队列加以处理，并按事先设定的带宽、缓冲处理输出队列，最后按 PHB 所指定的丢弃策略对 IP 包实施必要的丢弃。

④ 核心路由器将只依据 DSCP 字段为业务流选择特定的 PHB，根据 PHB 所指定的排队策略，将属于不同业务类别的业务流导入不同的队列加以处理，并按事先设定的带宽、缓冲处理输出队列，最后按 PHB 所指定的丢弃策略对 IP 包实施必要的丢弃。

DiffServ 的优点如下：

- DiffServ 最主要的优势是弱化了对信令的依赖，中间节点只需依据一定的分组标记应用各种 PHB 即可，无须像 IntServ 在每个路由器上为每个业务流保留“软状态”，避免了大量的资源预留信息的传递，具有更好的可扩展性。
- DiffServ 不要求实现端到端的 QoS 保证，只要求在 DS 域内 QoS 的一致性，而在 DS 域之间进行一定的映射来保证不同类别业务的 QoS。
- DiffServ 将 QoS 的一致性范围缩小到每个区域之中，从而降低了这种模型实现的复杂性。
- DiffServ 模型的绝大部分分类和整形操作只在 DS 域的边缘路由器上执行，大大简化了在 DS 域内核心路由器对传输 IP 包的操作。而 IntServ 模型需要在传输的整个路由中对每个 IP 包都进行相应的分类和整形操作。

DiffServ 的缺点如下：

DiffServ 不提供全网端到端的 QoS 保证，它所提供的 QoS 只是一种相对的 QoS 只是不同等级业务流之间的 QoS 好坏关系，在转发方式上仍然是采用传统 IP 网的逐跳转发方式。有关业务等级的具体划分、每类业务性能的量化描述、IP 业务类别与 ATM QoS 的映射等技术细节，IETF 还未给出具体的规定。

3）MPLS

MPLS（Multi-Protocol Label Switching，多协议标记交换技术）是一种利用给每个分组打上的固定标记，在开放的通信网络上用硬件对分组进行转发的高速、高效传输的新技术。这种采用硬件技术对打上标记的分组进行转发称为标记交换。另外，MPLS 并不仅限于使用 ATM，它可以使用多种链路层协议，如 IPX，DECnet，PPP，以太网以及帧中继等，所以，这种标记交换是“多协议”的。

MPLS 协议的关键是引入了标记（label）的概念。它是一种固定长度的、短的、不包含拓扑信息、只具有局部意义的信息内容。Label 短是为了易于处理，通常可以用索

引直接引用。只具有局部意义是为了便于分配。

MPLS 的作用如下：

- 在无连接的网络中引入连接模式从而减少了网络的复杂性。
- 兼容现有各种主流网络技术，能大大降低网络成本。
- 在提高 IP 业务性能的同时，能确保网络通信的服务质量和数据传输的安全性。

MPLS 的基本术语如下：

- 标记交换路由器 LSR。

标记交换路由器 LSR 具有标记交换和路由选择两种功能。因为它使用标记交换功能对分组进行转发。在转发分组前它需要使用路由选择功能构造分组转发表。根据标记交换协议确定特定标记的路径，即标记交换路径 LSP。而 LSR 是根据 LSP 来构造分组转发表的。

- 转发等价类 FEC。

所有需要做相同转发处理（具有同样服务类别和同样丢弃优先级）并转发到相同下一跳的分组属于同一转发类。如：目的 IP 地址与某一个特定 IP 地址的前缀匹配的分组，所有源地址与目的地址都相同的分组，具有某种服务质量需求的分组。相同 FEC 的分组都指派同样的标记，所以入口节点并不是给每一个分组指派一个不同的标记。而且 FEC 和标记是一一对应的。

- 标记栈。

MPLS 的一个重要功能就是可以构成标记栈，如图 1-98 所示。

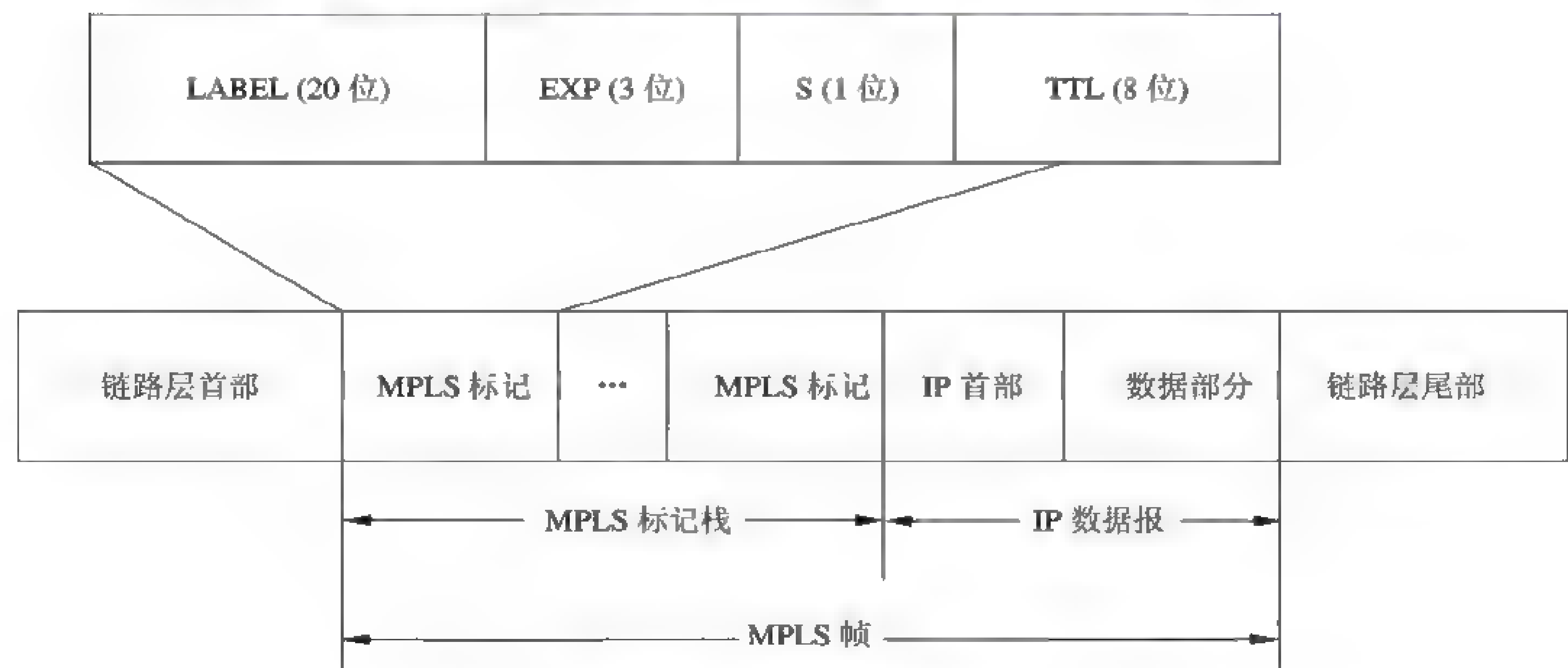


图 1-98　MPLS 的标记和标记栈

MPLS 标记一旦产生就压入到标记栈中，而整个标记栈放在数据链路层首部和 IP 首部之间。栈是一种后进先出的数据结构。MPLS 协议规定，标记栈的栈顶（最后进入栈

的标记）最靠近数据链路层首部，而栈底最靠近 IP 首部。在最简单的情况下，标记栈中只有一个标记。

MPLS 的基本工作过程如下：

- MPLS 域中的各 LSR 使用专门的标记分配协议 LDP 交换报文，并找出标记交换路径 LSP。各 LSR 根据这些路径构造出分组转发表。
- 分组进入到 MPLS 域时，MPLS 入口节点把分组打上标记，并按照转发表将分组转发给下一个 LSR。
- 以后的所有 LSR 都按照标记进行转发。每经过一个 LSR，要换一个新的标记。

当分组离开 MPLS 域时，MPLS 出口节点把分组的标记去除。再以后就按照一般分组的转发方法进行转发。

1.8.2 传输层协议 TCP 与 UDP

TCP 和 UDP 是 Internet 传输层的两个协议。从图 1-79 可以看出它们分别为应用层的不同协议提供服务。当然什么样的应用层协议使用 TCP，什么样的应用层协议使用 UDP，是根据它们的需要及 TCP 和 UDP 的特点而决定的。

1．TCP 协议特点

TCP 是面向连接的协议，提供可靠的、全双工的、面向字节流的、端到端的服务。

TCP 的连接是一对端点的连接，为了清晰地表明这条连接的源地址和目的地址，给每一个端点分配一个套接字（socket）或插口。虽然每台主机对端口号是独立编号，但是 IP 地址是唯一的，和 IP 地址绑定后所形成的插口就是唯一的。

套接字=（IP 地址：端口号）

端口号对应主机中的一个应用进程，编程语言通常用 port 表示。由此可得：

TCP 连接：：=（Socket1,Socket2）=（(IP1:port1），(IP2:port2)）

2．TCP 报文格式

TCP 报文格式如图 1-99 所示。

- 序号：4 字节。TCP 传送的数据流每一个字节都编有一个序号。序号字段中的值是本报文段所发送数据的第一个字节的序号。
- 确认号：4 字节。确认字段的值是期望收到对方下一个报文段的数据的第一个字节的序号。
- 数据偏移：4 字节。它指出当前 TCP 报文段的数据起始处距离 TCP 报文段的起始处有多远。“数据偏移”的单位不是字节而是 32 bit 字（4 字节为计算单位）。
- 紧急比特 URG：当 URG = 1 时，表明紧急指针字段有效。
- 确认比特 ACK：只有当 ACK = 1 时确认号字段才有效。
- 推送比特 PSH：接收 TCP 收到推送比特置 1 的报文段，就尽快地交付给接收应用进程，而不再等到整个缓存都填满了后再向上交付。

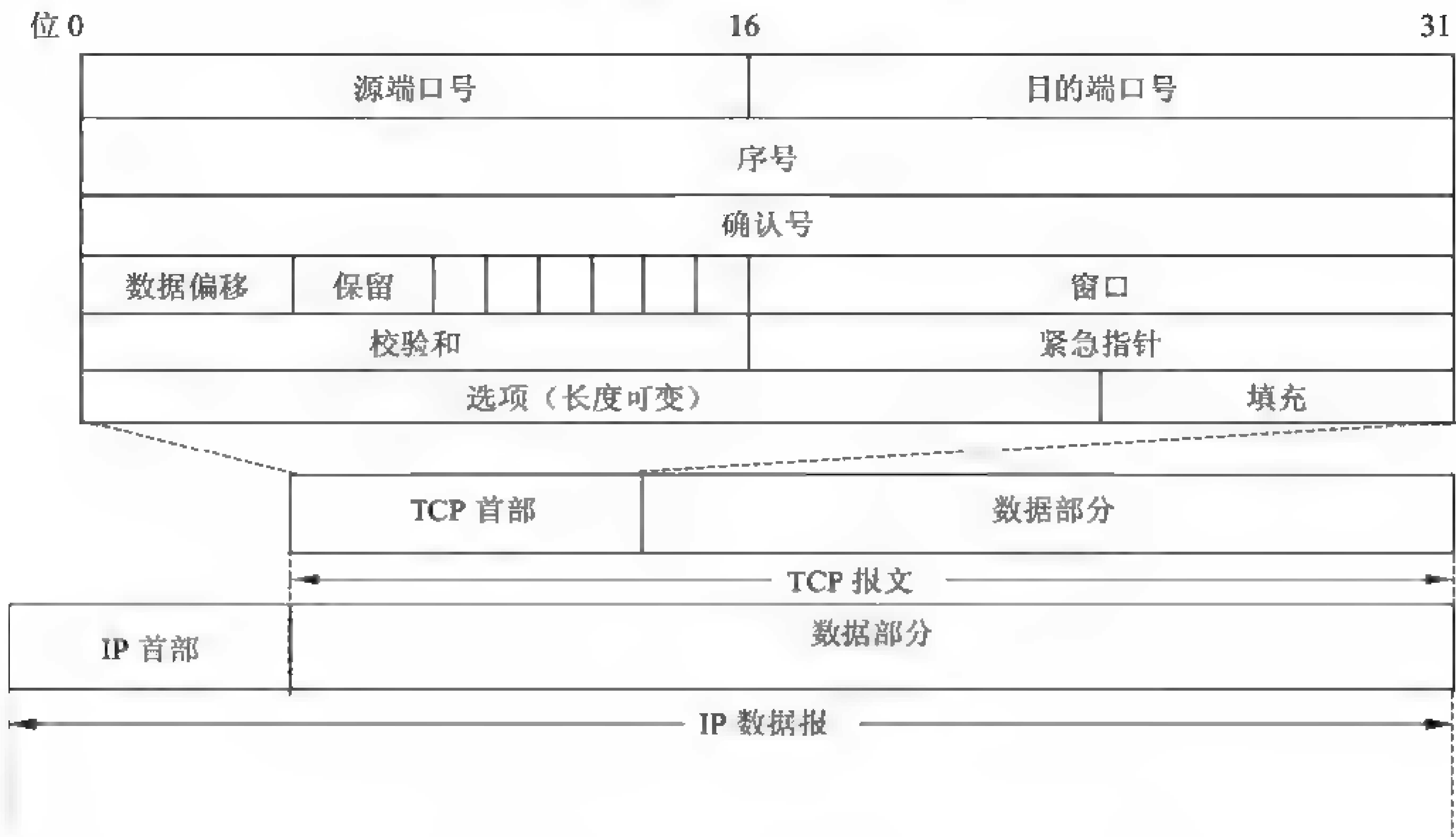


图 1-99　TCP 报文的格式及它与 IP 数据报的关系

- 复位比特 RST：当 RST = 1 时，表明 TCP 连接中出现严重差错（如由于主机崩溃或其他原因），必须释放连接，然后再重新建立运输连接。
- 同步比特 SYN：同步比特 SYN 置为 1，就表示这是一个连接请求或连接接受报文。
- 终止比特 FIN：用来释放一个连接。当 FIN = 1 时，表明此报文段的发送端的数据已发送完毕，并要求释放运输连接。
- 窗口：2 字节。窗口字段用来控制对方发送的数据量。TCP 连接的一端根据设置的缓存空间大小确定自己的接收窗口大小，然后通知对方以确定对方的发送窗口的上限。

3．TCP 建立与释放连接机制

TCP 提供的可靠服务，在连接的建立和释放上也体现了出来。

1）TCP 连接建立机制

TCP 使用三次握手来建立连接，大大增强了可靠性。如防止已失效的连接请求报文段到达被请求方，产生错误造成资源的浪费。

具体过程如图 1-100 所示。

2）TCP 连接释放机制

TCP 的释放分为：半关闭和全关闭两个阶段。半关闭阶段是当 A 没有数据再向 B 发送时，A 向 B 发出释放连接请求，B 收到后向 A 发回确认。这时 A 向 B 的 TCP 连接就关闭了。但 B 仍可以继续向 A 发送数据。当 B 也没有数据再向 A 发送时，这时 B 就

向 A 发出释放连接的请求，同样，A 收到后向 B 发回确认。至此为止 B 向 A 的 TCP 连接也关闭了。当 B 确实收到来自 A 的确认后，就进入了全关闭状态，如图 1-101 所示。

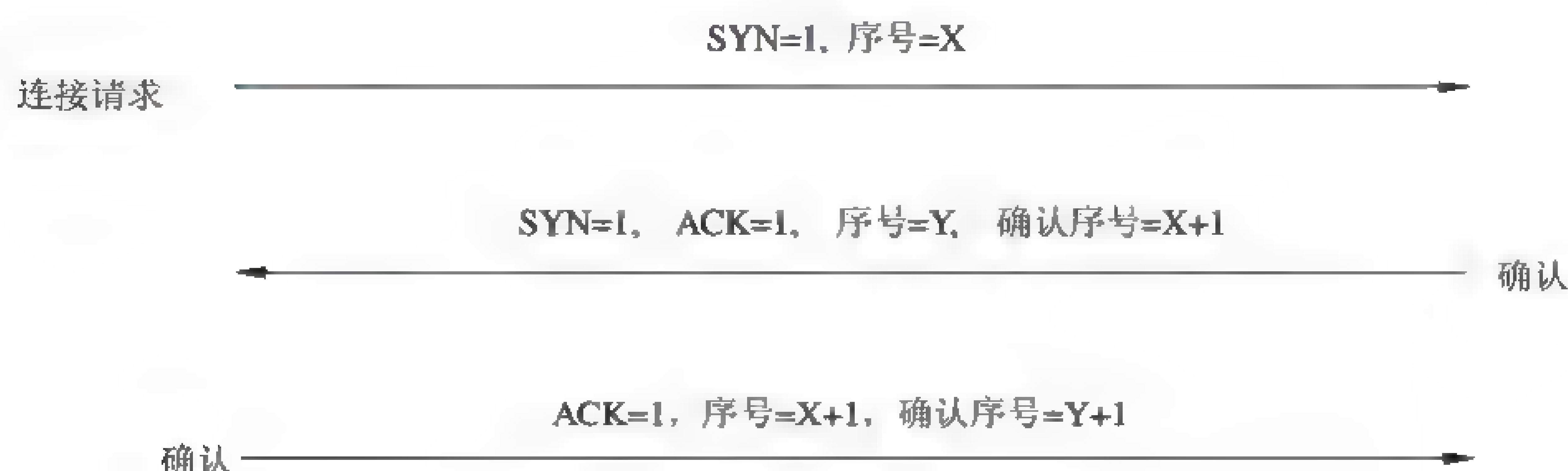


图 1-100 TCP 三次握手连接建立过程

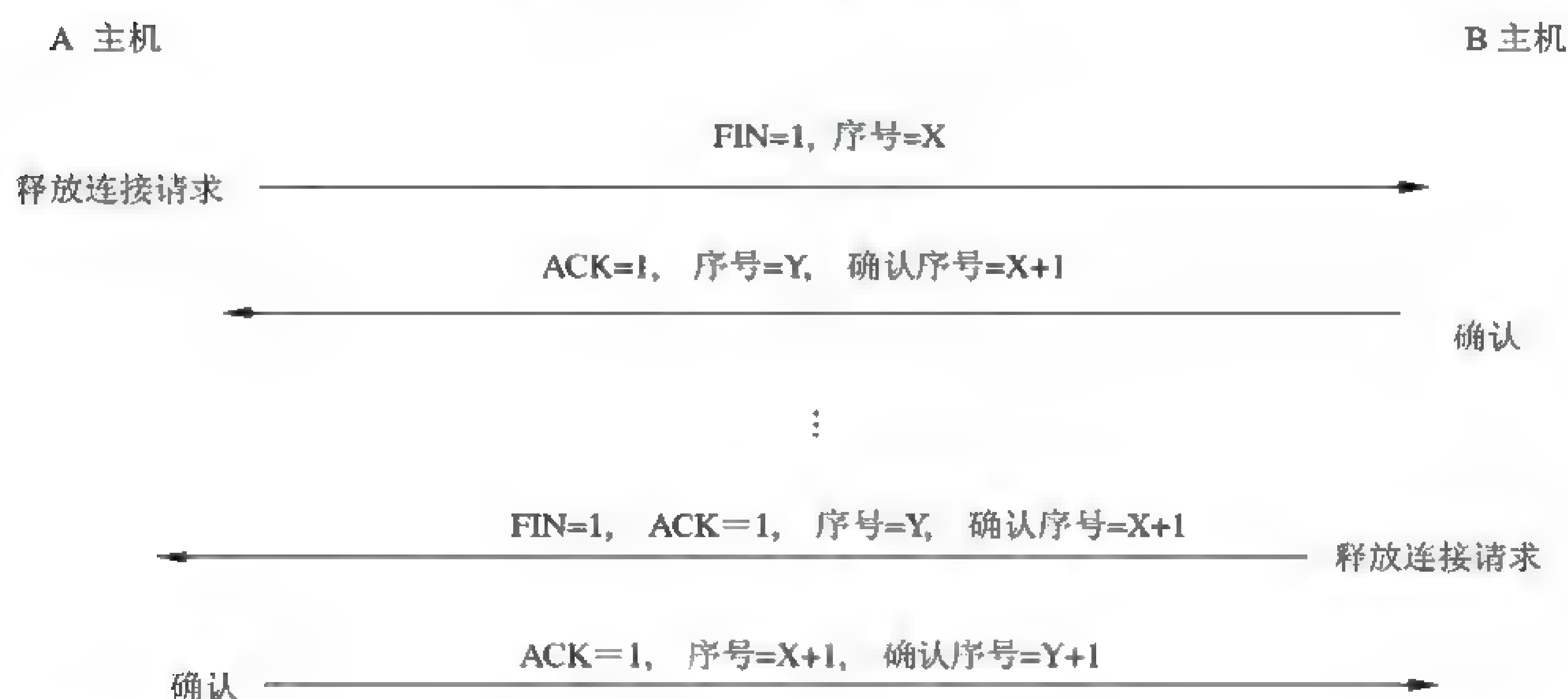


图 1-101 TCP 释放连接的过程

4．TCP 定时管理机制

重传机制是保证 TCP 可靠性的重要措施。TCP 每发送一个报文段，就对这个报文段设置一次计时器。只要计时器设置的重传时间到但还没有收到确认，就要重传这一报文段。超时重传时间设置的长短、恰当与否关系到网络的工作效率。如果设置得太短，会引起很多报文段的重传，增大网络的负荷；如果设置得太长，则会增大网络的空闲时间，降低网络的传输效率。

TCP 采用如下方法计算超时重传时间。

所涉及的参数：报文段的往返时间 RTT，报文段的加权平均往返时延 RTTs，超时重传时间 RTO，RTT 的偏差的加权平均值 RTT_D。

具体步骤如下：

首先计算出来第一个 RTT。然后把第一个 RTT 值设置为 RTTs 的初始值。以后再计算新的 RTTs 时采用如下公式：

$$新的\ RTTs=(1-\alpha)\times(旧的\ RTTs)+\alpha\times(新的\ RTT\ 样本)$$

其中α的值常取为 1/8。计算 RTO 的公式为：

$$RTO=RTTs+4\times RTT_D$$

RTT_D 的初始值为 RTT 样本值的一半，以后再计算 RTT_D 时采用公式：

$$新的\ RTT_D=(1-\beta)\times(旧的\ RTT_D)+\beta\times|RTTs-新的\ RTT\ 样本|$$

其中β的值常取为 1/4。

需要注意的是往返时间 RTT 的测量是比较复杂的。

5．TCP 拥塞控制策略

传输层的主要任务是保证端到端可靠的传输。端到端之间跨越的是若干个网络（局域网和广域网）。所以要保证网络高的传输效率，必须保证网络的畅通，不会发生拥塞现象。因为一旦网络发生拥塞，不但网络的传输速度会降低，而且还会导致数据的丢失和重传。那么网络在什么情况下会发生拥塞呢？可以把网络发生拥塞的条件用如下式子表示：

$$\sum 对资源的需求>可用资源$$

其中资源是指链路的容量、交换节点的缓存大小和处理机速度。

所谓拥塞控制就是防止过多的数据注入网络，使网络中的链路和交换节点（路由器）的负荷不致过载而发生拥塞。

发送端的主机在确定发送报文段的速率时，既要根据接收端的接收能力，又要从全局考虑不要使网络发生拥塞。因此，每一个 TCP 连接需要有接收端窗口和拥塞窗口两个状态变量，发送端的窗口取两者中较小的值。接收窗口就是 TCP 报文段首部中的窗口字段的值，是接收端主机根据其目前的接收缓存大小所许诺的最新的窗口值。拥塞窗口是网络的传输能力，是由发送端设置的。

TCP 的拥塞控制主要有以下 4 种方法：慢开始、拥塞避免、快重传和快恢复。

1）慢开始和拥塞避免

因为当主机开始发送数据时，如果立即将较大的发送窗口中的全部数据字节都注入到网络，由于还不清楚网络的状况，有可能引起网络拥塞。经验证明，较好的方法是试探一下，即由小到大逐渐增大发送端的拥塞窗口数值，就是所谓的慢开始算法。

慢开始的工作过程（如图 1-102 所示）：通常在刚刚开始发送报文段时可先将拥塞窗口 cwnd 设置为一个最大报文段 MSS 的数值。而在每收到一个对新的报文段的确认后，将拥塞窗口增加至多一个 MSS 的数值。用这样的方法逐步增大发送端的拥塞窗口 cwnd，可以使分组注入到网络的速率更加合理。

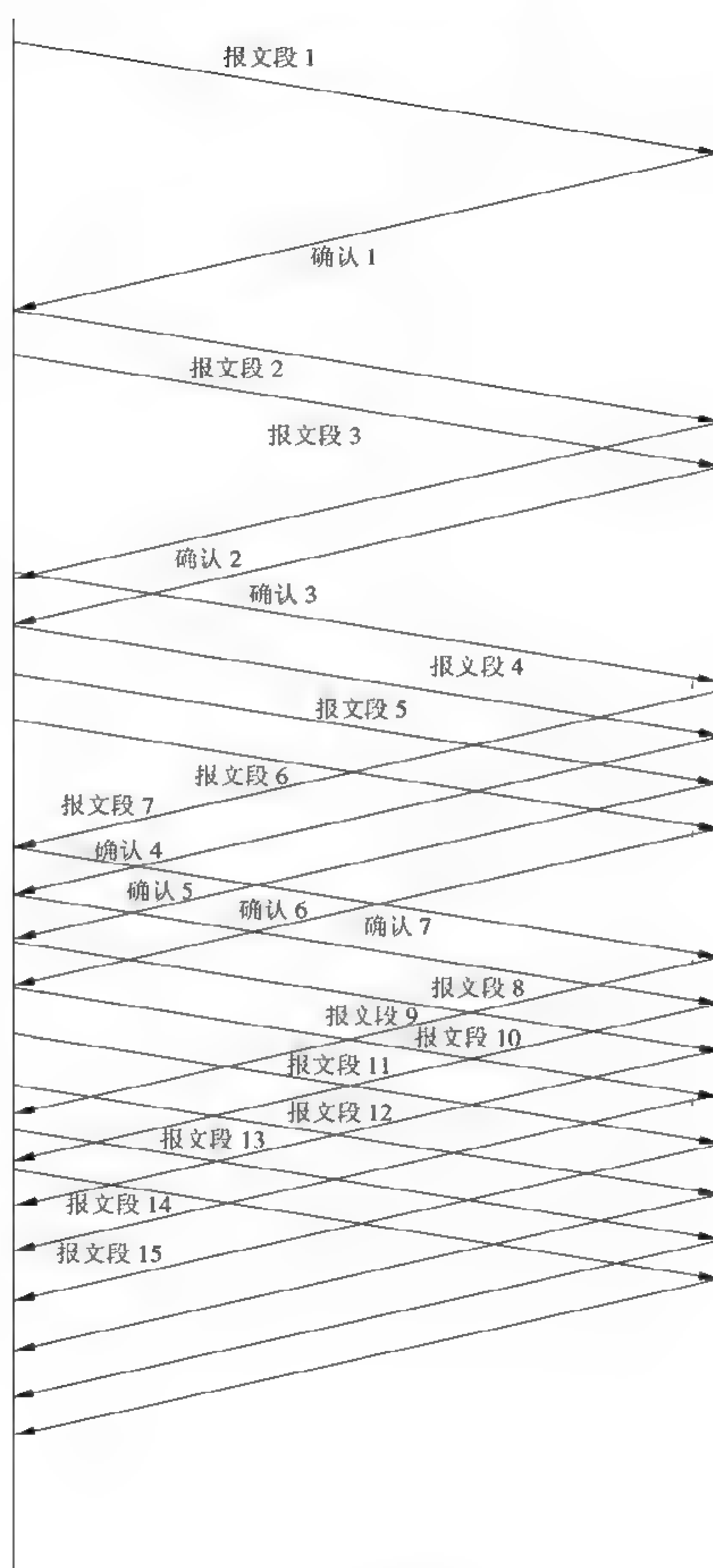

报文段 1
确认 1
报文段 2
报文段 3
确认 2
确认 3
报文段 4
报文段 5
报文段 6
报文段 7
确认 4
确认 5
确认 6
确认 7
报文段 8
报文段 9
报文段 10
报文段 11
报文段 12
报文段 13
报文段 14
报文段 15

图 1-102 慢开始算法

当然，在这种机制下，拥塞窗口也不会一直成指数增长，通常会设置一个慢开始门限值 ssthresh，当拥塞窗口达到此值时，就变为线性增长，执行拥塞避免算法。在整个过程中一旦出现数据传输超时，就会把拥塞窗口重新回到 1，并再次开始慢开始算法。

2）快重传和快恢复

快重传和快恢复是 TCP 拥塞控制机制中为了进一步提高网络性能而设置的两个算法。

快重传算法规定，发送端只要一连收到三个重复的 ACK 即可断定有分组丢失了，就应立即重传丢失的报文段而不必继续等待为该报文段设置的重传计时器的超时，如图 1-103 所示。不难看出，快重传并非取消重传计时器，而是在某些情况下可更早地重传丢失的报文段，从而提高吞吐率。

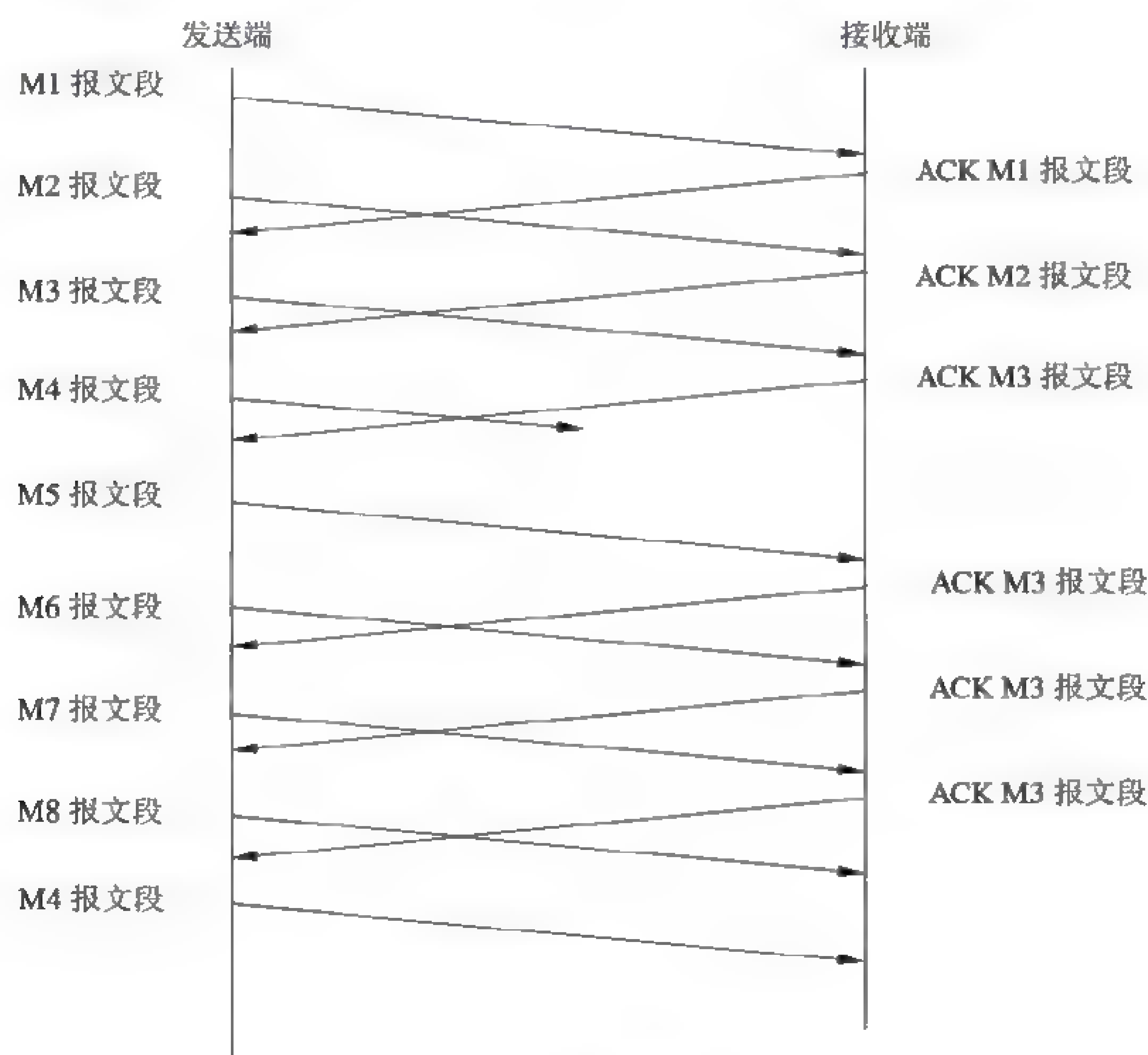


图 1-103　快重传算法

快恢复算法是和快重传算法相配合的算法。在采用快恢复算法时，慢开始算法只是在 TCP 连接建立时和网络出现超时时才使用。其工作要点为：当发送方连续收到三个重复的报文段确认时，就把慢开始门限值缩小一半，并执行拥塞避免算法——线性增加拥塞窗口。

3）随机早期检测 RED

TCP 拥塞管理的另一种方法是预防性分组丢弃。使用这种方法，路由器在输出缓存完全装满之前，即网络发生拥塞之前，准确地说是在检测到网络拥塞的早期征兆时（路由器的平均队列长度超过一定的门限值），就丢弃一个或多个分组，以便改进网络的性能。预防性分组丢弃的最重要的例子是随机早期检测。

（1）随机早丢弃 RED 产生的背景。

因为当网络上出现拥塞时，路由器的缓存由于充满而开始丢弃分组。对于 TCP 通信量，这是进入慢开始阶段的一个信号。但在这种情况下有两个困难：

① 丢失的分组必须重传，这又增加了网络的负荷，并导致 TCP 流增加了明显的时延。

② 全局同步的现象。由于出现拥塞而丢弃很多分组。可能出现的结果是有许多的 TCP 连接受到影响，接着进入了慢开始。这样会引起网络通信量的急剧下降，所以在一段时间内，网络处在不必要的低利用率的状况。因为许多 TCP 连接在大约同一时刻进入慢开始，它们也将在大约同一时刻脱离慢开始，而这将引起另一个大的突发和另一个“盛宴与饥荒”的循环。

（2）随机早丢弃 RED 算法。

RED 算法，路由器在输出缓存完全装满之前，就随机丢弃一个或多个分组，避免了发生全局性拥塞的现象，使得拥塞控制只是在个别的 TCP 连接上进行。

在这个算法中，路由器的队列维持两个参数，即队列长度最小门限 THmin 和最大门限 THmax。RED 对每一个到达的数据报都先计算平均队列长度 LAV。

① 若平均队列长度小于最小门限 THmin，则将新到达的数据报放入队列进行排队。

② 若平均队列长度超过最大门限 THmax，则将新到达的数据报丢弃。

③ 若平均队列长度在最小门限 THmin 和最大门限 THmax 之间，则按照某一概率 p 将新到达的数据报丢弃。

这里需要注意的关键问题是最小门限 THmin、最大门限 THmax 和概率 p 的选择。

6. 无线 TCP

由于移动计算机环境存在着 BER 高、带宽低、移动性及能量有限等特点，使得原本为固定主机、有线网络设计的 TCP 协议在这种环境下出现了很多不适应的问题。即使在拥塞控制机制不断改进的情况下，TCP 在无线网络中的传输性能仍无根本提高。针对无线网络的 TCP 方案大致可以划分为三类：

- 端到端方案（end-to-end scheme）。
- 分段连接方案（split connection scheme）。
- 数据链路层方案（link-layer scheme）。

端到端方案需要对 TCP 协议进行修改，由 TCP 发送端对传输过程中发生的不同错误进行处理，使得发送端能有效处理各种移动环境下造成的数据包丢失。分段连接方案

通过在基站终止 TCP 连接而对有线网络隐藏无线链路。这种方案通过在基站将源端和目的端的 TCP 连接分为两个独立的部分来实现。也就是一个 TCP 连接是在有线网络和基站之间，另一个 TCP 连接是在基站和移动设备之间。第一个连接使用的是传统的 TCP 协议；第二个 TCP 连接也就是无线链路上的连接可以使用经过修改的 TCP 协议，从而增强处理无线链路上各种错误的能力。数据链路层方案的目的是通过将局部重传（local retransmission）机制和前向错误纠正（Forward Error Correction，FEC）机制结合起来以对 TCP 源端隐藏各种和无线链路相关的分组丢失。

1）端到端方案

端到端方案需要对 TCP 协议进行修改，由 TCP 发送端对传输过程中发生的不同错误进行处理，使得发送端能有效处理各种移动环境下造成的数据包丢失。这种方案的目的是使 TCP 发送端能够区分拥塞相关的数据包丢失和其他形式的数据包丢失。只有当网络拥塞发生时，TCP 拥塞控制处理过程才被激活，而对于其他形式的丢包则执行其他错误恢复处理过程。

传输协议的核心问题是错误控制问题，包括错误检测和错误恢复问题。端到端方案中的错误检测可以分为两大类：隐式错误检测和显式错误通知。在错误恢复过程中采取对不同的丢包原因采取不同的恢复办法。

这种端到端方案的优点是保持了 TCP 的端到端语义（semantics）。缺点是需要对固定网络主机上的 TCP 算法进行改动，并且如果要对 Internet 上现存的所有 TCP 应用进行修改是一件及其困难的事情。

2）分段连接方案

分段连接方案通过在基站终止 TCP 连接而对有线网络隐藏无线链路。这种方案通过在基站将源端和目的端的 TCP 连接分为两个独立的部分来实现。也就是一个 TCP 连接是在有线网络和基站之间，另一个 TCP 连接是在基站和移动设备之间。第一个连接使用的是传统的 TCP 协议；第二个 TCP 连接也就是无线链路上的连接可以使用经过修改的 TCP 协议，从而增强处理无线链路上各种错误的能力。

这种方案是基于局部问题局部解决的思想，也就是由于无线/移动的原因造成的错误应该对固定主机（源端）屏蔽，从而无须修改固定主机上的 TCP 协议。

分段连接方案由于基站维持了两段连接，因此必须缓冲大量的状态信息，包括连接控制信息和未确认数据包。当业务量很大时，基站的负荷会变得非常重，而且需要更大的缓冲区。如果移动设备频繁地切换，基站之间状态信息的传输会带来较大时延，导致丢包。

3）数据链路层方案

数据链路层方案的目标是通过在无线链路上进行重传或错误纠正来屏蔽不可靠的

无线链路对有线网络的影响。其优点是可以独立于高层协议而提高数据传输的可靠性，并且无须保留每次连接的状态信息。目前常用的两种链路层纠错技术为：前向错误纠正（FEC）及自动重传请求（ARQ）技术。当丢包不是很频繁并且时延不是很敏感时，ARQ是一种非常有效的方法：缺点是可能会和 TCP 重传机制互相影响。FEC 的优点是发送时包含了一些冗余信息，以便能够恢复损毁的包，这对于时延较长的情况非常有利，而且FEC 不会和 TCP 的重传机制相互影响。FEC 的缺点是信道利用率不高，并且还需要额外花费时间和存储空间。

7. UDP 协议

1）UDP 的特点

UDP 只在 IP 的数据报服务之上增加了很少一点的功能，即端口的功能和差错检测的功能。虽然 UDP 用户数据报只能提供不可靠的交付，但 UDP 在某些方面有其特殊的优点：

- 发送数据之前不需要建立连接。
- UDP 的主机不需要维持复杂的连接状态表。
- UDP 用户数据报只有 8 个字节的首部开销。
- 网络出现的拥塞不会使源主机的发送速率降低。这对某些实时应用是很重要的。

TCP 协议和 UDP 协议的应用如表 1-9 所示。

表 1-9 TCP 协议和 UDP 协议的应用

应　　用	应用层协议	运输层协议
名字转换	DNS	UDP
文件传送	TFTP	UDP
路由选择协议	RIP	UDP
IP 地址配置	BOOTP，DHCP	UDP
网络管理	SNMP	UDP
远程文件服务器	NFS	UDP
IP 电话	专用协议	UDP
流式多媒体通信	专用协议	UDP
多播	IGMP	UDP
电子邮件	SMTP	TCP
远程终端接入	TELNET	TCP
万维网	HTTP	TCP
文件传送	FTP	TCP

2）UDP 用户数据包的首部格式

UDP 数据包格式如图 1-104 所示。

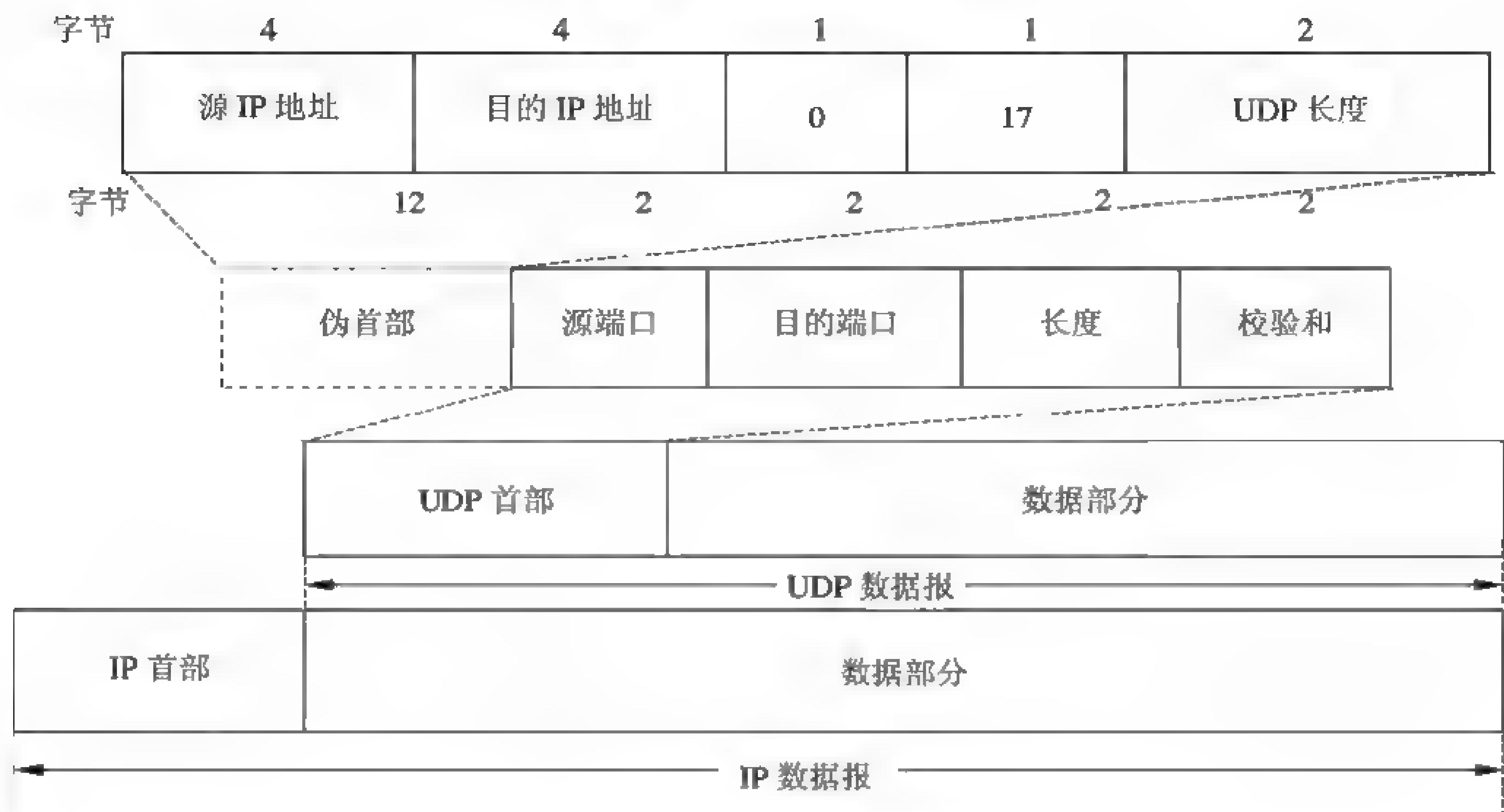


图 1-104　UDP 数据包及它与 IP 数据包的关系

1.8.3　应用层协议

每个应用层协议都是为了解决某一类应用问题，而问题的解决又往往是通过位于不同主机中的多个应用进程之间的通信协同工作来完成的。应用层的具体内容就是规定应用进程在通信时所遵循的协议。

1.8.3.1　域名系统（DNS）

域名系统 DNS 的功能是把 Internet 中的主机域名解析为对应的 IP 地址。域名系统 DNS 是一个联机分布式数据库系统。工作方式采用客户服务器方式。域名服务器是运行域名服务器程序的机器。

1．DNS 名字空间

目前，因特网的命名方法是层次树状结构的方法。采用这种命名方法，任何一个连接在因特网上的主机或路由器，都有一个唯一的层次结构的名字，即域名(domain name)。域是名字空间中一个可被管理的划分。域可以继续划分为子域，如二级域、三级域等等。域名的结构由若干个分量组成，各分量之间用点（请注意，是小数点的点）隔开：

…．三级域名．二级域名．顶级域名

各分量分别代表不同级别的域名。

每一级的域名都由英文字母和数字组成（不超过 63 个字符，并且不区分大小写字母），完整的域名不超过 255 个字符。

目前顶级域名（Top Level Domain，TLD）有国家顶级域名、国际顶级域名、通用顶级域名三大类。最早的顶级域名是：.com 表示公司企业、.net 表示网络服务机构、.org 表示非赢利性组织、.edu 表示教育机构（美国专用）、.gov 表示政府部门（美国专用）、.mil 表示军事部门（美国专用）。

图 1-105 是因特网名字空间的结构图。

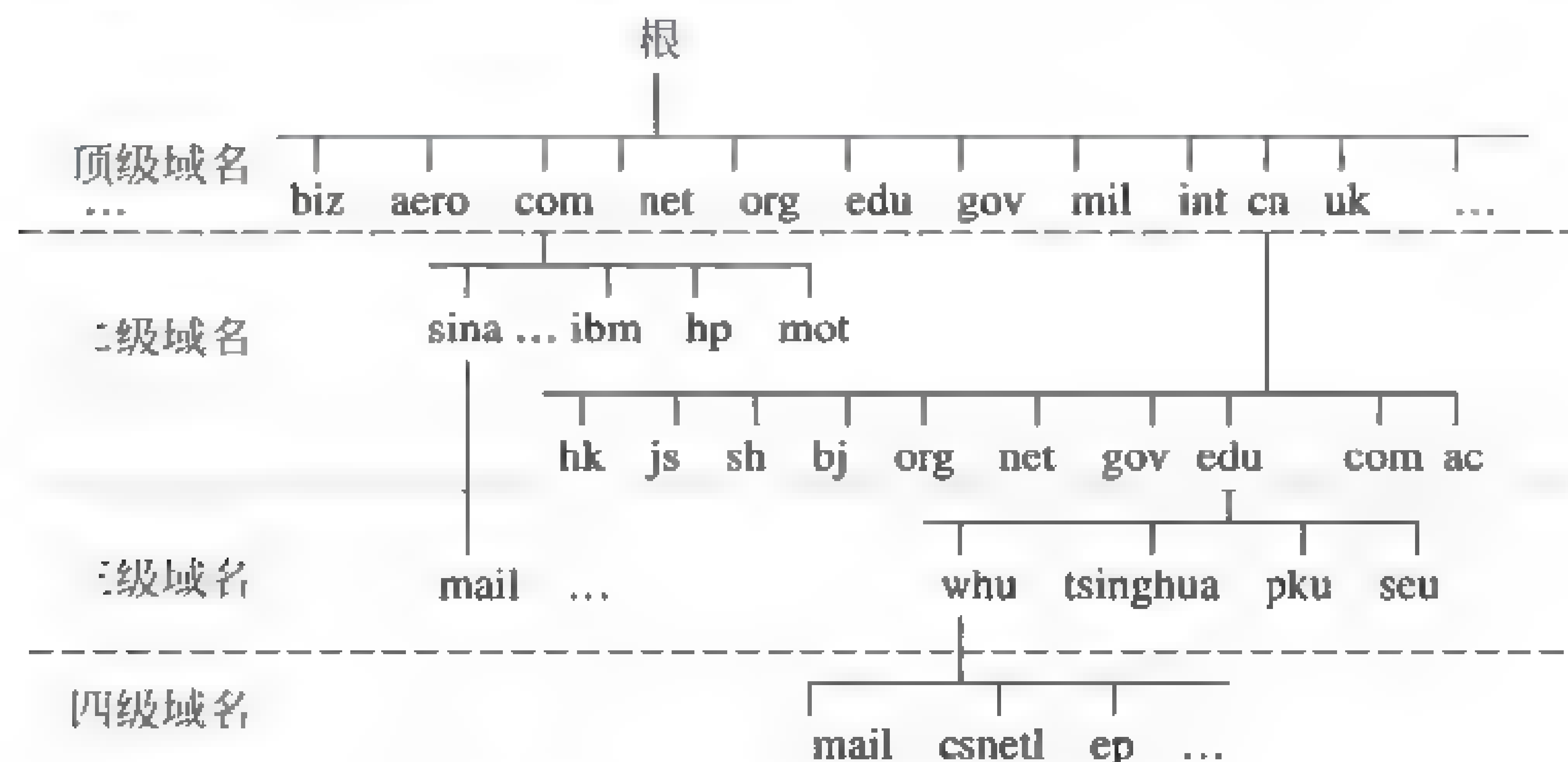


图 1-105 因特网的名字空间

要强调指出的是，因特网的名字空间是按照机构的组织来划分的，与物理的网络无关，与 IP 地址中的“子网”也没有关系。

2．资源记录

DNS 资源记录语法：

{name} {TTL} addr-class record-type record-specific-data

- name：域记录的名字。通常只有第一个 DNS 资源记录配置 name 栏，对于区域文档中其他的资源记录，name 也可能是空白，这种情况下，其他的资源记录接受先前的资源记录的名字。
- TTL：Live 栏可选择的时间。指定该数据在数据库中保管多长时间，此栏为空表示默认的生存周期在授权资源记录开始中指定。
- addr-class：地址类。大范围用于 Internet 地址和其他信息的地址类为 IN。
- record-type：记录类型。常为 A NS MX CNAME。
- record-specific-data：记录类型的数据。

record-type 的定义如表 1-10 所示。

表 1-10 record-type 的定义

类 型	意 义	值
SOA	StartofAuthority	该区的参数
A	主的 IP 地址	32 位整数
MX	邮件交换	优先权，域

续表

类　型	意　义	值
NS	名字服务器	本域服务器名
CNAME	规范名	域名
PTR	指针	IP 地址的别名
HINFO	主机描述	CPU、OS 信息
TXT	文本	ASCII 串

3．域名服务器

可以把域名服务器分为根域名服务器、顶级域名服务器、权限域名服务器和本地域名服务器4种不同类型。

（1）根域名服务器（root name server）：根域名服务器是最高层次的域名服务器。每一个根域名服务器都要存有所有顶级域名服务器的IP地址和域名。当一个本地域名服务器对一个域名无法解析时，就会直接找到根域名服务器，然后根域名服务器会告知它应该去找哪一个顶级域名服务器进行查询。目前全世界共有一百多个根域名服务器，这样做的目的是满足本地域名服务器就近查找，从而提高DNS查询的速度和合理利用Internet的资源。

（2）顶级域名服务器（TLD server）：顶级域名服务器负责管理在本顶级域名服务器上注册的所有二级域名。当收到 DNS 查询请求时，能够将其管辖的二级域名转换为该二级域名的IP地址。或者是下一步应该找寻的域名服务器的IP地址。

（3）权限域名服务器（authoritative name server）：DNS采用分区的办法来设置域名服务器。一个服务器所管辖的范围称为区。区的范围小于或等于域的大小。各个单位可以根据自己单位的情况来划分区的范围。每一个区都设置有服务器，这个服务器叫权限服务器，它负责将其管辖区内的主机域名转换为该主机的IP地址。在其上保存有所管辖区内的所有主机域名到IP地址的映射。

（4）本地域名服务器（local name server）：也称为默认域名服务器。当一个主机发出DNS查询报文时，这个查询报文就首先被送往该主机的本地域名服务器。当选择PC中“Internet协议（TCP/IP）”的“属性”，就可看到DNS地址的选项。其中的DNS服务器就是本地域名服务器。本地域名服务器离用户较近，一般不超过几个路由器的距离。当所要查询的主机也属于同一个本地ISP时，该本地域名服务器立即就能将所查询的主机名转换为它的IP地址，而不需要再去询问其他的域名服务器。

4．域名解析

域名解析过程的要点：当某个应用进程需要把某个主机的域名解析为对应的IP地址时，它将调用解析程序，成为DNS的客户方，并把要解析的主机域名放在DNS请求报文中，然后使用 UDP 用户数据报将其发往本地域名服务器。本地域名服务器对其进行对应查询，如果查找成功，就将结果放入DNS回答报文中，同样使用UDP用户数据报

将返回给请求方。

需要再次强调的是各种服务器之间的查询都是以客户服务器方式进行的。

在域名的解析过程中，本地域名服务器可以采用递归查询和迭代查询两种查询方式。

递归查询的思想：当某个主机有域名解析请求时，它总是首先向本地域名服务器发出查询请求，如果本地域名服务器知道查询结果，那么它将把结果返回给请求者；如果本地域名服务器不知道查询结果，它将作为DNS客户方向根域名服务器发出查询请求。然后由根域名服务器去完成接下来的查询。图1-106给出了一个递归查询的例子。在这个例子中主机whu.edu.cn要查询域名为dry.ssd.com的IP地址。

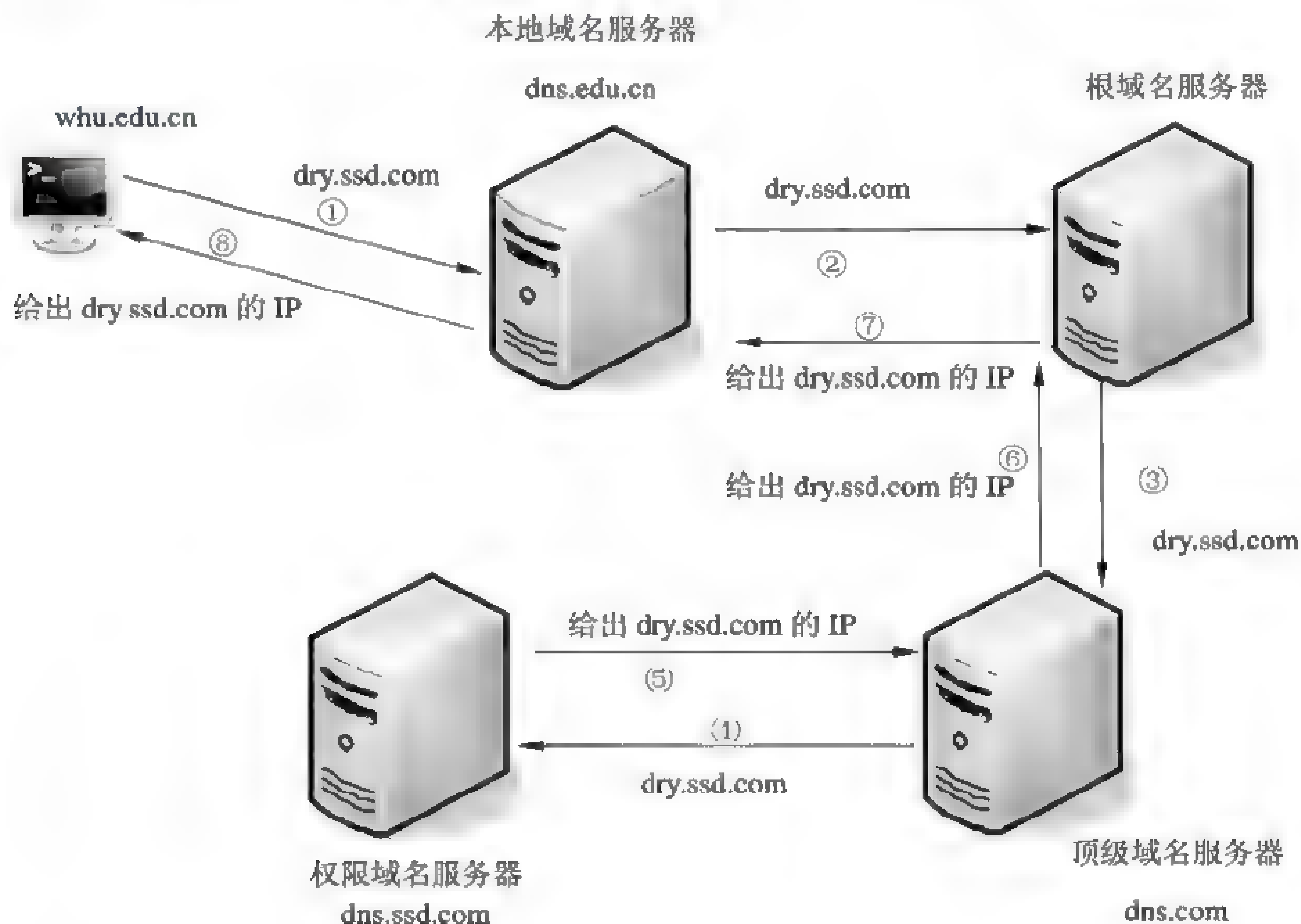


图1-106 本地域名服务器的递归查询

迭代查询的思想：当根域名服务器收到本地域名服务器的查询请求时，它根据查询请求告诉本地域名服务器下一步应该去查询的顶级域名服务器的IP地址；接着本地域名服务器到该顶级域名服务器进行查询，若顶级域名服务器能够给出查询结果，那么它会把结果传送给本地域名服务器，否则它会告诉本地域名服务器下一步应该查询的权限域名服务器的IP地址；本地域名服务器就这样迭代进行查询，直到最后查到了所需要的IP地址，然后把结果反馈给发起查询的主机。图1-107给出了一个迭代查询的例子。同样还是主机whu.edu.cn要查询域名为dry.ssd.com的IP地址。

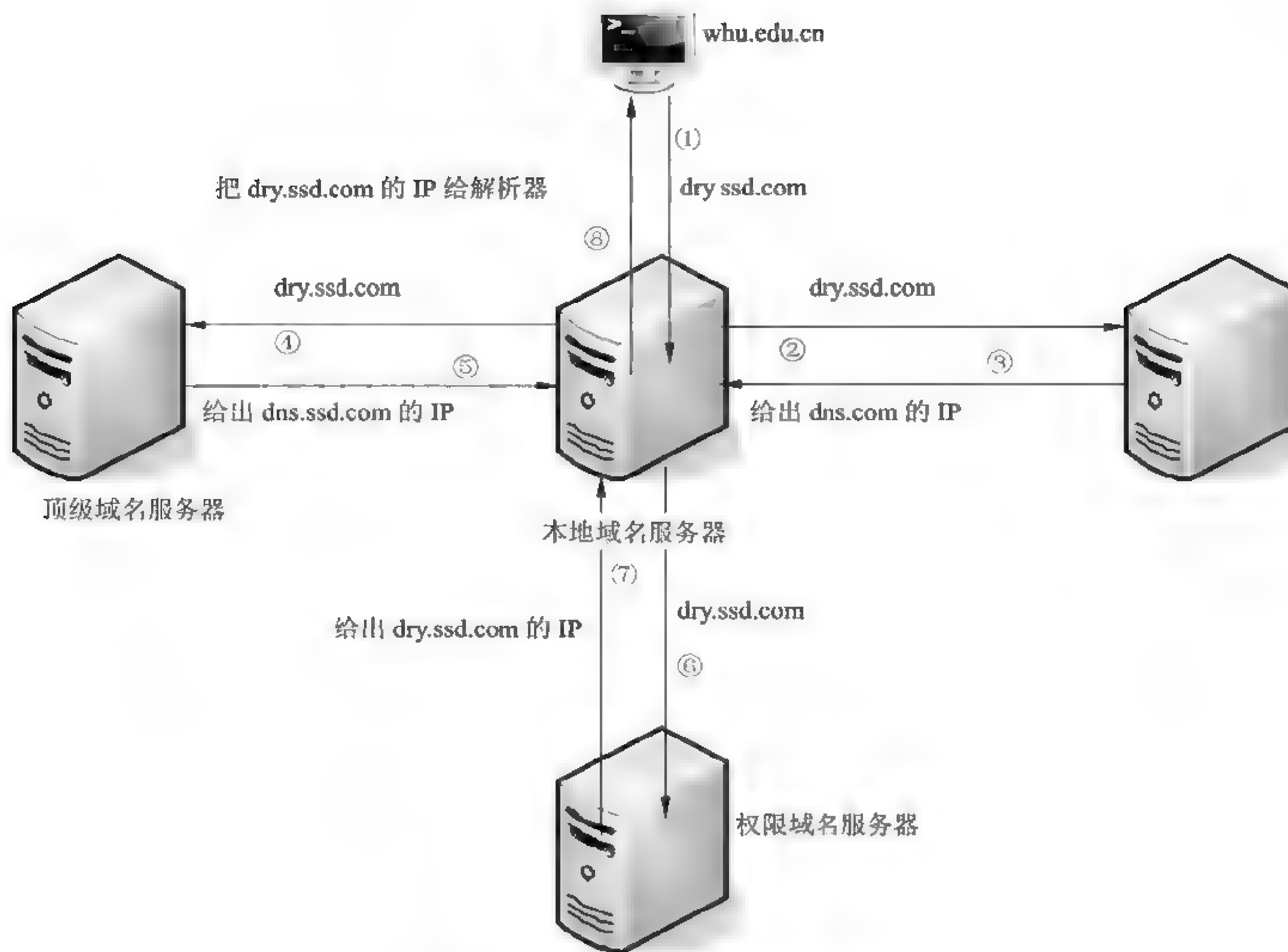


图 1-107　本地域名服务器采用迭代查询

另外，在域名服务器中常常使用高速缓存来提高 DNS 的查询效率。 主机和每个域名服务器都维护一个高速缓存，存放最近查询过的域名以及从何处获得域名映射信息的记录。当有域名解析请求时，首先在自己的高速缓存中查找，若没有才向其他域名服务器求助。为了维护最新的高速缓存中的记录，高速缓存中的记录隔一段时间还要进行清除处理。

5. DNS 报文格式

报文由 12 字节的首部和 4 个长度可变的字段组成（如图 1-108 所示）。标识字段由客户程序设置并有服务器返回结果。

QR：0 表示查询报文，1 表示响应报文。

Opcode：通常值为 0（标准查询），其他值为 1（反向查询）和 2（服务器状态请求）。

AA：表示授权回答（authoritative answer）。

TC：表示可截断的（truncated）。

RD：表示期望递归。

RA：表示可用递归。

随后 3bit 必须为 0。

Rcode：返回码，通常为 0（没有差错）和 3（名字差错）。

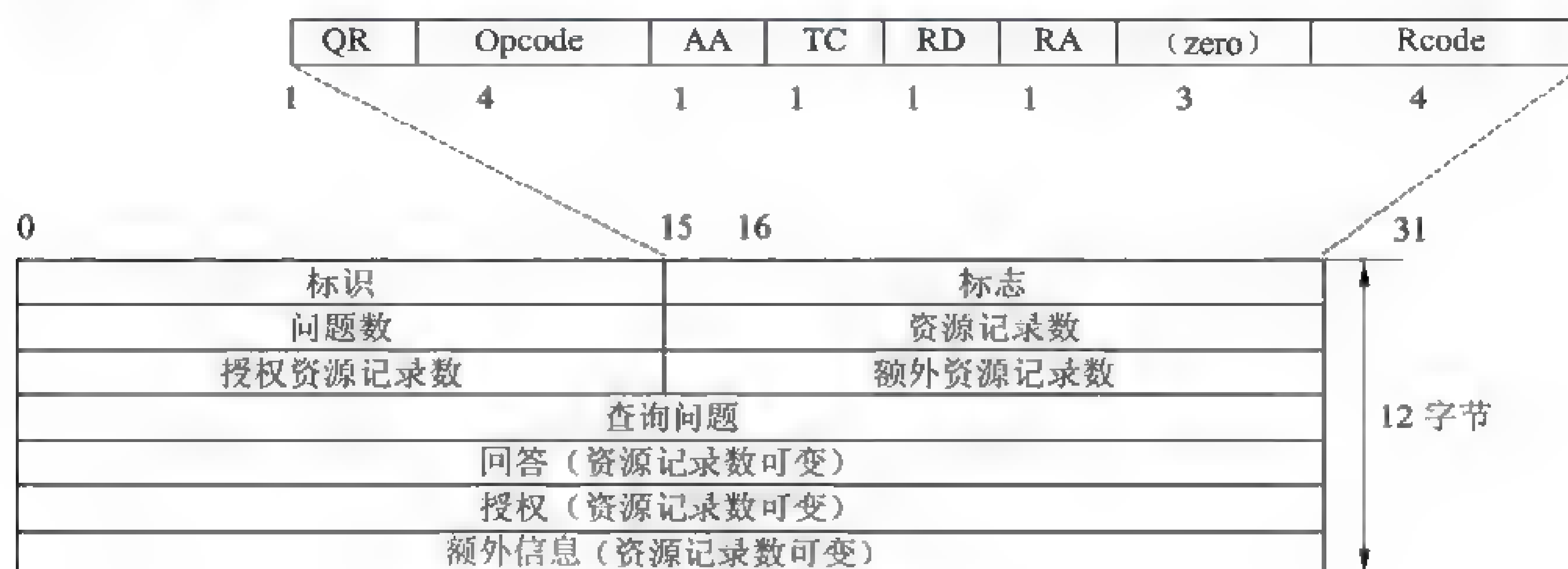


图 1-108 DNS 的报文格式

1.8.3.2 电子邮件协议

电子邮件（E-mail）是因特网上使用得最多的和最受用户欢迎的一种应用。电子邮件将邮件发送到 ISP 的邮件服务器，并放在其中的收信人邮箱（mail box）中，收信人可随时上网到 ISP 的邮件服务器进行读取。电子邮件不仅使用方便，而且还具有传递迅速和费用低廉的优点。现在电子邮件不仅可传送文字信息。而且还可附上声音和图像。

1. 邮件系统功能

电子邮件系统的主要功能包括撰写、显示、处理、传输和报告 5 项基本功能。其中撰写、显示、处理是用户代理至少应当具有的三个功能，而传输和报告是邮件服务器应该具备的功能。

- 撰写：给用户提供很方便地编辑信件的环境。
- 显示：能方便地在计算机屏幕上显示出来信（包括来信附上的声音和图像）。
- 处理：处理包括发送邮件和接收邮件。收信人应能根据情况按不同方式对来信进行处理。例如，阅读后删除、存盘、转发等，对于不愿收的信件可直接在邮箱中删除。
- 传输：包括发送和接收。发送是把邮件从邮件发送者的 PC 中发送到本地邮件服务器，以及从本地邮件服务器传送到目的邮件服务器的过程。接收是把邮件从目的邮件服务器传送到接收邮件用户的 PC 中的过程。
- 报告：是邮件服务器向发信人报告邮件传送的情况。如已发送成功、发送失败等。

2. 体系结构

体系结构中包括用户代理、邮件服务器、消息传输代理和邮件协议（如图 1-109 所示）。

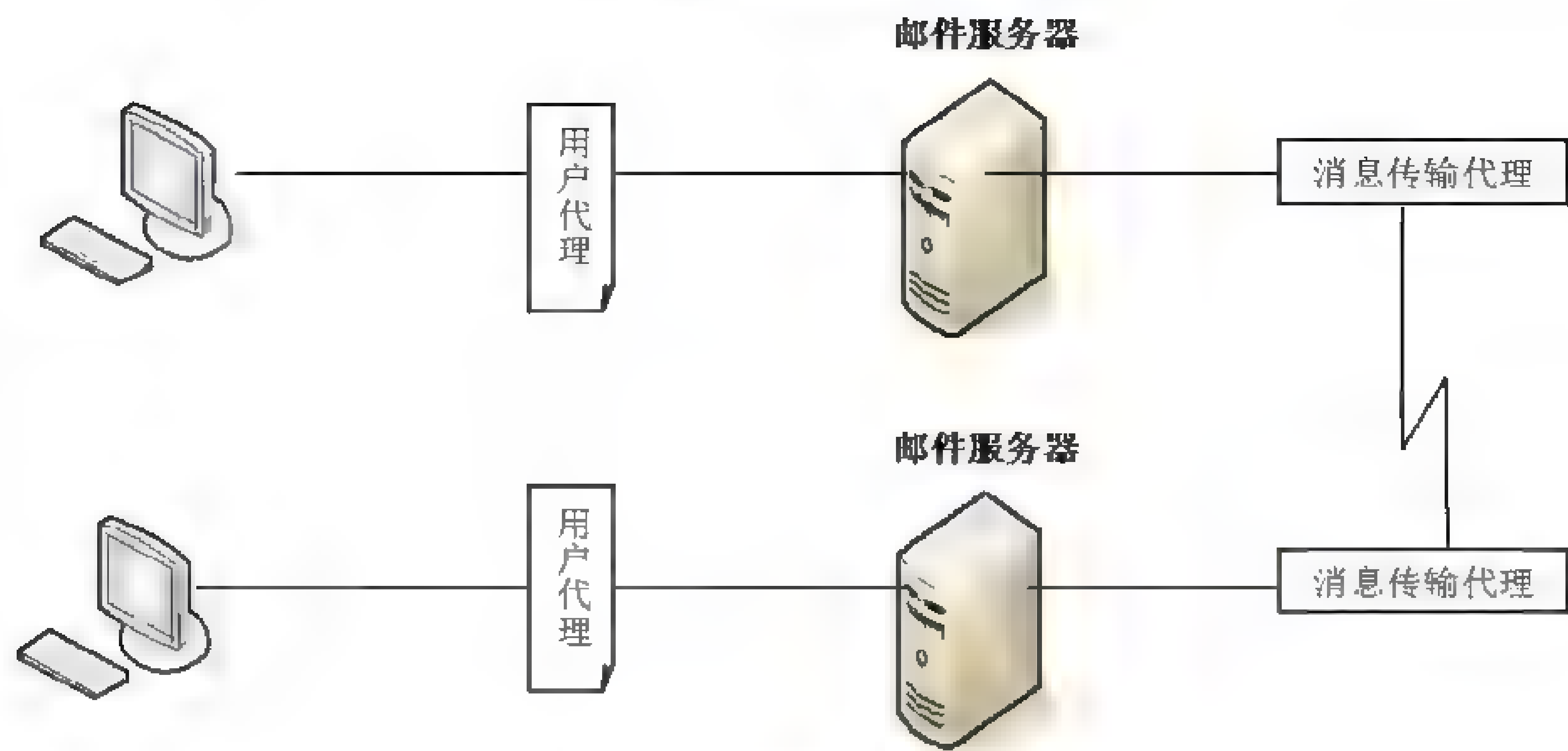


图 1-109　邮件系统体系结构

用户代理的功能前面已经讲过，邮件服务器的功能是用于存储邮件，这里消息传输代理的功能就是实现前面所说的传输和报告，邮件协议有发送协议 SMTP、接收协议 POP3/IMAP4。关于邮件协议的功能在下面内容叙述。

3. 邮件格式

一个电子邮件分为信封、首部和主体（正文），首部和主体也称为内容部分。首部需要用户填写，首部写好后邮件系统将自动地将信封所需的信息提取出来并写在信封上。所以用户不需要填写电子邮件信封上的信息。邮件的主体部分由用户自由撰写。

（1）RFC 822 对邮件的首部格式做了规定，如表 1-11 所示。

表 1-11　RFC 822 邮件头所用的一些关键词

关　键　字	含　　义
TO:	第一收信人的电子邮件地址
Cc:	第二收信人的电子邮件地址
From:	撰写邮件的个人或多个名字
Sender:	实际发信人的电子邮件地址
Date:	发送邮件的日期和时间
Reply-To:	回信应送达的电子邮件地址
Subject:	在一行中显示一个邮件的简短摘要
Keywords:	用户选择的关键词
Bcc:	盲抄送的电子邮件地址

（2）邮件正文。

最简单的内容编码就是 7 位 ASCII 码（SMTP 只能传送这种编码），而且每行不能超过 1000 个字符。

用户在撰写邮件时一般都是使用自己最熟悉的语言文字，但是这种文本不能被SMTP传送，而且二进制文件和可执行文件同样也不能被SMTP传送。

但是在通用Internet邮件扩充MIME中定义了传送非ASCII码的编码规则。MIME的内容传送编码规则有Base64和Quoted-printable encoding。

Base64编码：适用于传送任意的二进制文件。具体编码规则如下：

第一步，将二进制代码划分为一个个24bit长度的单元。

第二步，将每一个24bit单元划分为4个6bit组。每一个6bit组按以下方法转换成ASCII码。6bit的二进制代码共有64种不同的值（0～63）。

先排大写字母：A表示0，B表示1……

再排小写字母：a 表示26，b表示27……

再排10个数字：0表示52，1表示53……

最后+表示62，/表示63。

例：有二进制代码：00110100 01000100 11001000

解：先划分为4个6bit 分组：

	001101	000100	010011	001000
对应的Base64编码：	N	E	T	8
最后要传送的ASCII：	01001110	01000101	01010100	00001000

Quoted-printable 编码：适用于当所传送的数据中只有少量的非 ASCII 码。“=”和不可打印的ASCII码以及非ASCII码的数据的编码规则为：先将每个字节的二进制代码用两个十六进制数字表示，然后在前面加上一个“=”，简单地说就是ASCII码大于127的字符替换为“=”及两个十六进制数。“=”的Quoted-printable编码为“3D”。

例如：武汉的二进制编码为：11001110 11100100 10111010 10110101

对应的十六进制编码：	CE	E4	BA	BA
Quoted-printable 编码：	3DCE	3DE4	3DBA	3DBA

4．邮件发送与接收协议

1）SMTP发送协议

SMTP的工作方式也是客户服务器的方式。负责发送邮件的SMTP进程就是SMTP客户，负责接收邮件的 SMTP 进程是 SMTP 服务器。它在传输层使用 TCP 协议进行传输。

SMTP规定在两个相互通信的SMTP进程之间应如何交换信息。

它规定了14条命令和三类应答信息。每条命令用4个字母组成。

① SMTP命令集。

HELO：发送身份标识。

MAIL：识别邮件发起方。

RCPT：识别邮件接收方。

DATA：传送报文文本。

RSET：放弃当前邮件事物。

NOOP：无操作。

QUIT：关闭 TCP 连接。

SEND：向终端发送邮件。

SOML：若可能向终端发送邮件，否则发往信箱。

SAML：向终端和信箱发送邮件。

VRFY：证实用户名。

EXPN：返回邮件发送清单的成员。

HELP：发送帮助文档。

TURN：颠倒发送方和接收方的角色。

② SMTP 应答码包括肯定、暂时否定、永久否定三大类。

③ 建立连接。

第一步，使用 SMTP 的熟知端口号码（25）与目的主机的 SMTP 服务器建立 TCP 连接（不使用中间服务器）。

第二步，接收程序通过应答 220 标识自己就绪。

第三步，发送程序发送 HELO 标识自己。

第四步，SMTP 服务器若有能力接收邮件，则回答“250 OK”，表示已准备好接收。若 SMTP 服务器不可用，则回答“421 Service not available（服务不可用）”。

④ 传送。

第一步，用一个 MAIL 命令标识报文发起方。

第二步，用一个或多个 RCPT 命令标识报文的接收方。

第三步，用一个 DATA 命令传送报文文本。

⑤ 释放连接。

第一步，发送一个 QUIT 命令，并等待应答。

第二步，关闭 TCP 连接。

2）接收协议

（1）POP3。

POP3 也使用客户服务器的工作方式。在接收邮件的用户 PC 中必须运行 POP 客户程序，而在用户所连接的 ISP 的邮件服务器中则运行 POP3 服务器程序。POP3 服务器具有身份鉴别功能，用户只有输入鉴别信息后才允许对邮箱进行读取，另外它还具有从服务器读取邮件并存放到本地机器上以及对邮件删除、备份等其他操作功能。

POP3 也使用 TCP 协议，对邮件进行传输。

POP3 协议的一个特点就是只要用户从 POP 服务器读取了邮件，POP 服务器就将该邮件删除了。

（2）IMAP。

IMAP 是一个联机协议。当用户 PC 上的 IMAP 客户程序打开 IMAP 服务器的邮箱时，用户就可看到邮件的首部。用户打开某个邮件时，那个邮件才传到用户的计算机上。所以用户可以在不同的地方使用不同的计算机反复阅读自己的邮件，直到用户发出删除邮件的命令，IMAP 服务器邮箱中的邮件会一直保存着。

5．邮件保密

电子邮件中有时会有一些非常隐私的东西，但电子邮件在传输过程中除了必须到达的邮件服务器外，还经常需要多个路由器进行转发，所以邮件的保密问题就成为一个值得考虑的问题。

1）PGP 协议

PGP 协议是 1995 年开发的。虽然不是 Internet 的正式标准，但已被广泛使用。PGP 的功能包括加密、鉴别、电子签名和压缩等技术。这些功能保证了电子邮件的安全性、报文完整性和发送方鉴别。下面通过一个例子来具体说明 PGP 的工作过程。

假定张三要想向李四发送安全电子邮件，使用 PGP 协议来保证其安全性。发送方张三应该有三个密钥：自己的私钥 K_{DA}，李四的公钥 K_{EB}，自己生成的一次性密钥 K。接收方李四需要两把密钥：自己的私钥 K_{DB} 和张三的公钥 K_{EA}。具体工作过程如下。

发送方张三的工作：

第一步，使用 MD5 对所发邮件的明文 M 进行摘要运算，结果为 H（M）。

第二步，张三使用自己的私钥 K_{DA} 对摘要 H（M）进行数字签名，结果为 E（H（M），K_{DA}）。

第三步，把 E（H（M），K_{DA}）和明文 M 拼接在一起，结果为 E（H（M），K_{DA}）+M。

第四步，张三使用自己生成的一次性密钥 K 对 E（H（M），K_{DA}）+M 进行加密，E（E（H（M），K_{DA}）+M，K）。

第五步，使用李四的公钥对张三的一次性私钥进行加密，结果为 E（K，K_{EB}）。

第六步，对 E（E（H（M），K_{DA}）+M，K）进行压缩，然后和 E（K，K_{EB}）一起发送给李四。

接收方李四的工作：

第一步，接收后，把压缩文件和 E（K，K_{EB}）进行分开，并对压缩文件进行解压缩。

第二步，李四用自己的私钥对 E（K，K_{EB}）进行解密，D（E（K，K_{EB}），K_{DB}）=K。

第三步，李四用密钥 K 对 E（E（H（M），K_{DA}）+M，K）进行解密，D（E（E（H（M），K_{DA}）+M，K））=E（H（M），K_{DA}）+M。

第四步，把 E（H（M），K_{DA}）+M 分开为 E（H（M），K_{DA}）和 M。

第五步，用张三的公钥对 E（H（M），K_{DA}）核实签名，得到结果 H（M）。

第六步，李四对明文 M 进行 MD5 的摘要运算，得到结果 h（M）。

第七步，比较 H（M）和 h（M）是否相等。如果相等证明电子邮件是张三发的。而且报文 M 没有被篡改，即报文的完整性得到检验。

2）PEM 协议

PEM 是因特网的邮件加密建议标准，由 4 个 RFC 文档来描述。

- RFC 1421：报文加密与鉴别过程。
- RFC 1422：基于证书的密钥管理。
- RFC 1423：PEM 的算法、工作方式和标识符。
- RFC 1424：密钥证书和相关的服务。

PEM 的功能和 PGP 的差不多，都是对基于 RFC 822 的电子邮件进行加密和鉴别。每个报文都是使用一次一密的方法进行加密，并且密钥也是放在报文中一起在网络上传送。对密钥还必须加密，可以使用 RSA 或三重 DES。PEM 有比 PGP 更完善的密钥管理机制。由证书管理机构（Certificate Authority）发布证书。

1.8.3.3　文件传输协议（FTP）

1．FTP 概述

FTP 的主要功能是减少或消除在不同操作系统下处理文件的不兼容性。

FTP 的主要作用就是让用户连接上一个远程计算机（这些计算机上运行着 FTP 服务器程序）查看远程计算机有哪些文件，然后把文件从远程计算机上复制到本地计算机，或把本地计算机的文件送到远程计算机去。

2．FTP 的工作过程

FTP 是一个交互会话的系统，在进行文件传输时，FTP 的客户和服务器之间需要建立两个 TCP 连接：控制连接和数据连接，如图 1-110 所示。

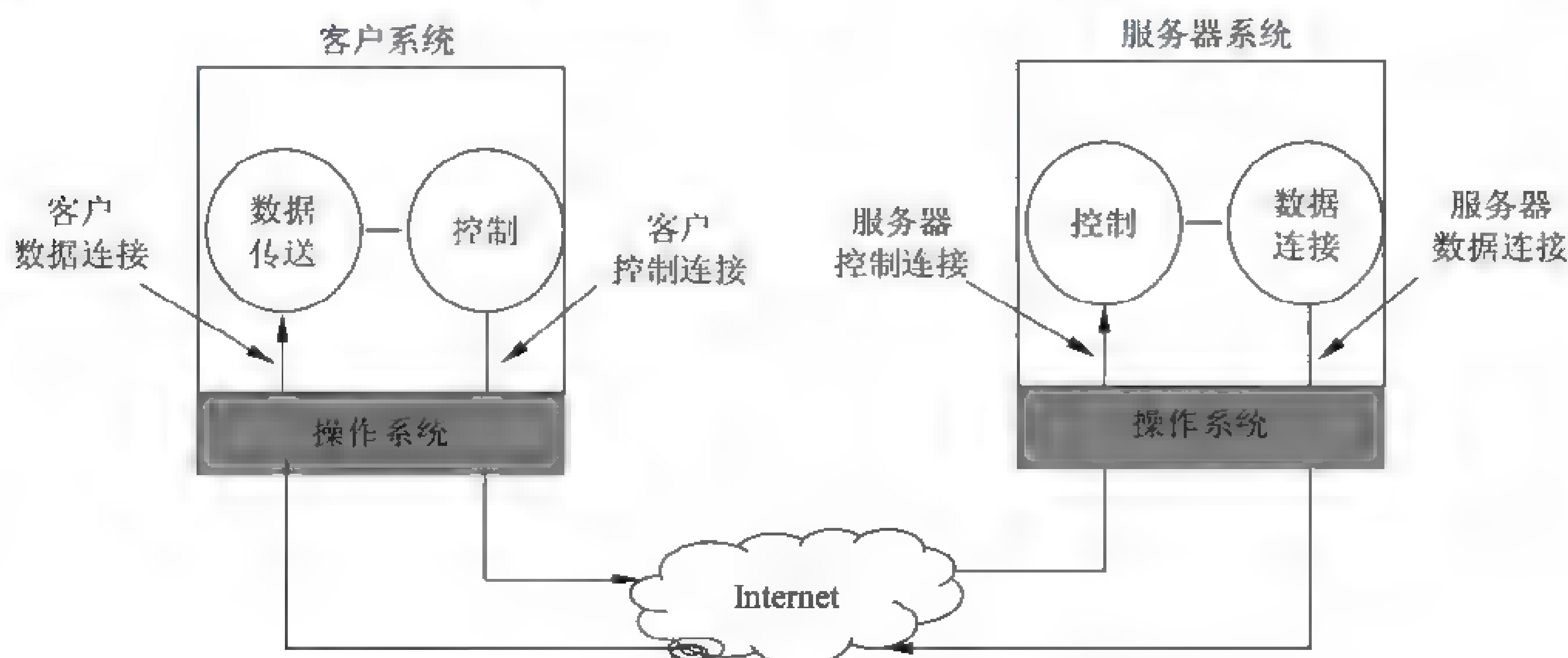


图 1-110　FTP 的两个 TCP 连接

控制连接在整个会话期间一直打开，FTP 客户发出的传送请求通过控制连接发送给服务器端的控制进程，但控制连接不用来传送文件。用于传输文件的是数据连接。服务器端的控制进程在接收到 FTP 客户发送来的文件传输请求后就创建数据传送进程和数据连接，用来连接客户端和服务器端的数据传送进程。数据传送进程在完成文件的传送后，关闭数据传送连接并结束运行。但控制连接并不一定关闭。

FTP 使用客户服务器方式，在传输层使用 TCP 可靠的服务。一个 FTP 服务器进程可同时为多个客户进程提供服务。FTP 的服务器进程由两大部分组成：一个主进程，负责接收新的请求；另外有若干个从属进程，负责处理单个请求。

（1）主进程的工作步骤（接收请求）如下：

① 打开端口 21。

② 监听客户的请求。

③ 收到请求后启动一个从属进程处理客户的请求；从属进程完成后自动终止。

④ 回到监听状态。

（2）从属进程的工作步骤如下：

① 接收主进程的命令，创建控制进程。

② 建立与客户的控制连接。

③ 收到客户从控制连接发来的传送请求后，创建数据传送进程。

④ 与客户建立数据连接（端口 20），并与数据传送进程关联。

⑤ 数据传送进程控制数据连接及其传送。

⑥ 传送完毕，释放数据连接，终止数据进程。

⑦ 释放控制连接，终止控制进程（一般由客户发起）。

主进程与从属进程的处理是并发进行的。

例如：一个主机 A 其 IP 地址为 202.114.4.6。假设主机 A 的 1500 进程向某个 FTP 服务器（IP 地址为 202.113.225.1）发出一个 FTP 连接请求。另外 1501 进程用来建立数据连接。FTP 服务器 21 号端口接收连接请求，分配从属进程 1600，接着插口（202.114.4.6:1500）和 FTP 服务器插口（202.113.225.1:1600）建立控制连接。同时把主机 A 的 1501 端口号通过控制连接传送给 FTP 服务器，FTP 服务器使用 20 号端口和该进程建立数据连接，接着插口（202.114.4.6:1501）和 FTP 服务器插口（202.113.225.1:20）建立数据连接。

上述例子仅仅是 FTP 工作在主动模式时的过程。其实 FTP 支持两种模式，一种方式叫做 Standard（也就是 PORT 方式，主动方式），一种是 Passive（也就是 PASV，被动方式）。Standard 模式 FTP 的客户端发送 PORT 命令到 FTP 服务器。Passive 模式 FTP 的客户端发送 PASV 命令到 FTP 服务器。

- Port 模式 FTP 客户端首先和 FTP 服务器的 TCP 21 端口建立连接，通过这个通道发送命令，客户端需要接收数据的时候在这个通道上发送 PORT 命令。PORT 命

令包含了客户端用什么端口接收数据。在传送数据的时候，服务器端通过自己的 TCP 20 端口连接至客户端的指定端口发送数据。FTP 服务器必须和客户端建立一个新的连接用来传送数据。

- Passive 模式在建立控制通道的时候和 Standard 模式类似，但建立连接后发送的不是 Port 命令，而是 Pasv 命令。FTP 服务器收到 Pasv 命令后，随机打开一个高端端口（端口号大于 1024）并且通知客户端在这个端口上传送数据的请求，客户端连接 FTP 服务器此端口，然后 FTP 服务器将通过这个端口进行数据的传送，这个时候 FTP 服务器不再需要建立一个新的和客户端之间的连接。

3．FTP 的命令

FTP 的命令主要有 get，put，mput，mget 和 ls 等等。

4．TFTP

TFTP 是一个很小且易于实现的文件传送协议。它的工作方式也采用客户服务器方式，但传输层使用 UDP 数据报，因此 TFTP 需要有自己的差错改正措施。

TFTP 只支持文件传输而不支持交互。TFTP 没有一个庞大的命令集，没有列目录的功能，也不能对用户进行身份鉴别。

TFTP 的主要特点：因为工作在停止等待方式，每个报文需要应答；UDP 报文固定 512B 长；可对文件进行读或写。

1.8.3.4　远程登录协议（Telnet）

Telnet 是 Internet 的登录和仿真程序。基本功能是，允许用户登录进入远程主机系统。目的是提供一个相对通用的，双向的，面向 8 位字节的通信机制。一个 Telnet 连接就是一个用来传输带有 Telnet 控制信息数据的 TCP 的连接。

1．基本服务

- Telnet 定义一个网络虚拟终端为远地系统提供一个标准接口。客户机程序不必详细了解远地系统，它们只需构造使用标准接口的程序。
- Telnet 包括一个允许客户机和服务器协商选项的机制，而且它还提供一组标准选项。
- Telnet 对称处理连接的两端，即 Telnet 不强迫客户机从键盘输入，也不强迫客户机在屏幕上显示输出。

2．工作过程

Telnet 远程登录服务分为以下 4 个过程：

- 本地与远程主机建立连接。该过程实际上是建立一个 TCP 连接，用户必须知道远程主机的 IP 地址或域名。
- 将本地终端上输入的用户名和口令及以后输入的任何命令或字符以 NVT（Net Virtual Terminal）格式传送到远程主机。该过程实际上是从本地主机向远程主机发送一个 IP 数据报。

- 将远程主机输出的 NVT 格式的数据转化为本地所接受的格式送回本地终端，包括输入命令回显和命令执行结果。
- 最后，本地终端对远程主机进行撤销连接。该过程是撤销一个 TCP 连接。

1.8.3.5 Web 应用与 HTTP 协议

1．Web 资源组织方式与 URL

WWW 是一种分布式的超媒体系统，它是超文本（hypertext）系统的扩充。一个超文本由多个信息源链接成。利用一个链接可使用户找到另一个文档。这些文档可以位于世界上任何一个接在因特网上的超文本系统中。超文本是万维网的基础。

WWW 基于客户/服务器模式，它改进了传统的客户/服务器计算模型，将原来客户端一侧的应用程序模块与用户界面分开，并将应用程序模块放到服务器上，形成基于 Web 浏览器的用户界面、应用程序和服务程序等三部分。这样应用程序可独立于客户端平台，使系统具有用户界面简单、地理、系统间的可移动、应用程序间可移植和可伸缩等优点。

WWW 使用统一资源定位符（Uniform Resource Locator，URL）来标识分布在整个 Internet 上的文档，所谓统一资源定位符就是用于完整地描述 Internet 上网页和其他资源的地址的一种标识方法。Internet 上的每一个网页都具有一个唯一的名称标识，通常称之为 URL 地址，这种地址可以是本地磁盘，也可以是局域网上的某一台计算机，更多的是 Internet 上的站点。URL 相当于一个文件名在网络范围的扩展。因此 URL 是与因特网相连的机器上的任何可访问对象的一个指针。

URL 采用相同的基本语法，无论寻址哪种特定类型的资源（网页、新闻组）或描述通过哪种机制获取该资源。语法如下：

[protocol]://hostname[:port]/path/[;parameters][?query]#fragment

参数说明如下。

- protocol（协议）：指定使用的传输协议，最常用的是 HTTP 协议，它也是目前 WWW 中应用最广的协议。
- hostname（主机名）：是指存放资源的服务器的域名系统（DNS）主机名或IP地址。
- :port（端口号）：整数，可选，省略时使用方案的默认端口，各种传输协议都有默认的端口号，如 http 的默认端口为 80。
- path（路径）：由零或多个“/”符号隔开的字符串，一般用来表示主机上的一个目录或文件地址。
- ；parameters（参数）：这是用于指定特殊参数的可选项。
- ？query（查询）：可选，用于给动态网页（如使用 CGI、ISAPI、PHP/JSP/ASP/ASP.NET等技术制作的网页）传递参数，可有多个参数，用“&”符号隔开，每个参数的名和值用“=”符号隔开。
- fragment：信息片断，字符串，用于指定网络资源中的片断。例如一个网页中有

多个名词解释，可使用 fragment 直接定位到某一名词解释。

2．Web 文档形式

World Wide Web 的最大好处之一就是能与成千上万的用户交互以获得和提供不同的信息。由于这种信息的动态本质，仅有静态的 HTML 页面是不够的，因此需要有一些方法来向访问 Web 站点的用户提供动态信息。

根据文档内容的确定时间，所有的 Web 文档可以划分为三类。

- 静态 Web 文档：静态 Web 文档是一个存在于 Web 服务器上的 HTML 文件，静态文档的作者在写作的时候决定文档的内容，由于文档的内容不会发生变化，所以对静态文档的每一次访问都返回相同的结果。
- 动态 Web 文档：动态 Web 文档不存在一个预先定义的格式，相反，动态文档在浏览器访问 Web 服务器时创建。当一个请求到达时，Web 服务器运行一个应用程序创建所需的动态 Web 文档，服务器返回程序的输出作为对浏览器请求的应答。由于每次访问都要创建新的文档，所以动态文档的内容是变化的。
- 活动 Web 文档：一个活动 Web 文档不完全由服务器一端规定，相反，一个活动 Web 文档可以包括一个计算和显示值的程序。当浏览器访问活动文档时，服务器返回一个浏览器可以执行的程序副本，返回以后，活动文档可以和用户交互执行并不停地改变显示。

3．超文本传输协议（HTTP）

1）重要术语

源服务器（origin server）：请求或者将要创建的资源所在的服务器。

代理服务器（proxy）：① 代理客户发出请求；② 代理源服务器应答。

连接：在两个应用程序之间建立的 TCP 连接。

Cache：存放被请求过的内容。

用户代理（user agent）：发出请求的客户程序。

实体：某个数据资源的特定表示或解释。

2）HTTP 协议工作原理

为了使超文本的链接能够高效率地完成，需要用 HTTP 协议来传送一切必须的信息。从层次的角度看，HTTP 是面向事务的（transaction-oriented）应用层协议，它使用 TCP 连接进行可靠的传送。HTTP 是一个无状态的协议，即服务器向客户机发送被请求的文件时，并不存储任何关于该客户机的状态信息。HTTP 协议定义了 Web 客户机是如何向 Web 站点请求 Web 页，以及服务器如何将 Web 页传送给客户机的。

3）HTTP 报文结构

① 请求报文格式如图 1-111 所示。

<table>
<tr><td>方法</td><td>空格</td><td>URL</td><td>空格</td><td>版本</td><td>请求行</td></tr>
<tr><td>首部字段名</td><td>:</td><td>空格</td><td colspan="2">值</td><td rowspan="3">首部行</td></tr>
<tr><td colspan="5">⋮</td></tr>
<tr><td>首部字段名</td><td>:</td><td>空格</td><td colspan="2">值</td></tr>
<tr><td colspan="5"></td><td>空行</td></tr>
<tr><td colspan="5">实体主体</td><td>实体主体部分</td></tr>
</table>

图 1-111 HTTP 请求报文格式

请求报文中有关信息如表 1-12 所示。

表 1-12 请求报文中有关信息

请求报文			
请求方式		请求首部字段	
OPTIONS	MOVE	Accept	If-Modified-Since
GET	DELETE	Accept-Charset	Proxy-Authorization
HEAD	LINK	Accept-Encoding	Range
POST	UNLINK	Accept-Language	Referer
PUT	TRACE	Authorization	Unless
PATCH	WRAPPED	From	User-Agent
COPY	Extension-method	Host	

例如：

```
GET/somedir/page.html HTTP/1.1
Host:www.someschool.edu
Connection:close
User-agent:Mozilla/4.0
Accept-languge:fr
```

② 响应报文格式如图 1-112 所示。

<table>
<tr><td>版本</td><td>空格</td><td>状态码</td><td>空格</td><td>短语</td><td>状态行</td></tr>
<tr><td>首部字段名</td><td>:</td><td>空格</td><td colspan="2">值</td><td rowspan="3">首部行</td></tr>
<tr><td colspan="5">⋮</td></tr>
<tr><td>首部字段名</td><td>:</td><td>空格</td><td colspan="2">值</td></tr>
<tr><td colspan="5"></td><td>空行</td></tr>
<tr><td colspan="5">实体主体</td><td>实体主体部分</td></tr>
</table>

图 1-112 HTTP 响应报文格式

响应报文中有关信息如表 1-13 所示。

表 1-13　响应报文中有关信息

响应报文			
响应状态码			响应首部字段
Continue	Moved Temporarily	Request Timeout	Location
Switching	See Other	Conflict	Proxy-Authenticate
Protocols	Not Modified	Gone	Public
OK	Use Proxy	Length Required	Retry-After
Created	Bad Request	Unless True	Server
Accepted	Unauthorized	Internal Server Error	WWW-Authenticate
Non -Authoritative	Payment Required	Not Implemented	
Information	Forbidden	Bad Gateway	
No Content	Not Found	Service Unavailable	
Reset Content	Method Not Allowed	Gateway Timeout	
Partial Content	None Acceptable	Extension code	
Multiple Choice	Proxy Authentication		
Moved	Required		
Permanently			

状态码都是三位数字，意义如下：

- 1xx 表示通知信息的，如请求收到了或正在进行处理。
- 2xx 表示成功，如接受或知道了。
- 3xx 表示重定向，表示要完成请求还必须采取进一步的行动。
- 4xx 表示客户的差错，如请求中有错误的语法或不能完成。
- 5xx 表示服务器的差错，如服务器失效无法完成请求。

例如：

```
HTTP/1.1  200  OK
Connection:close
Date: Thu, 03 Jul 2006 12:00:15 GMT
Server:Apache/1.3.0(Unix)
Last-Modified:Sun, 5 may 2006 09:23:24 GMT
Content-Length:6821
Content-Type:text/html
(data data data data …)
```

4．Cookie、Session 与 Web 缓存

开发网站涉及到页面间数据共享的时候，常常需要使用某一种方式来持久化我们的数据，持久化数据的方式有许多种，下面分别介绍 Application、Cookie、Session 和 Cache

这几种方式。

Cookie：提供了一种在 Web 应用程序中存储用户特定信息的方法。例如，当用户访问站点时，Cookie 存储用户首选项或其他信息。当该用户再次访问该网站时，便可以检索以前存储的信息。在开发人员以编程方式设置 Cookie 时，需要将希望保存的数据序列化为字符串（并且要注意，很多浏览器对 Cookie 有 4096B 的限制）然后进行设置。

Cookie 的关键特性有：存储于客户端硬盘上，与用户相关，在一定时间内持久化存储，可以跨浏览器共享数据，需要被序列化，发生服务器-客户端数据传输。

Session：为当前用户会话提供信息。还提供对可用于存储信息的会话范围的缓存的访问，以及控制如何管理会话的方法。存储在服务器的内存中，因此与在数据库中存储和检索信息相比，它的执行速度更快。会话状态应用于单个的用户和会话。

Session 的关键特性有：存储于服务器内存中，与会话相关，在会话的整个生存期中存在即不会被主动丢弃，不被序列化，不发生服务器-客户端数据传输。

Cache：存储于服务器的内存中，允许自定义缓存项以及将缓存多长时间。例如，当缺乏系统内存时，缓存会自动移除很少使用的或优先级较低的项以释放内存。该技术也称为清理，这是缓存确保过期数据不使用宝贵的服务器资源的方式之一。它不与会话相关，所以它是多会话共享的，因此使用它可以提高网站性能，但是可能泄露用户的安全信息。另外，在服务器缺乏内存时可能会自动移除 Cache，因此需要在每次获取数据时检测该 Cache 项是否还存在。

Cache 的关键特性有：存储于服务器内存中，与会话无关，根据服务器内存资源的状况随时可能被丢弃，不被序列化，不发生服务器-客户端数据传输。

综上所述，我们总结出一些常见而典型的例子。

电子商务网站的购物车：使用 Session，因为购物车信息是会话相关的而且安全性很重要。

论坛或其他网站的“记住我”功能：使用 Cookie，因为这是保存的往往只是一个用户名，而且当用户下次登录时还需要这个用户名仍然存在。

产品信息：Cache 是优先的选择，因为产品信息通常是与会话无关、修改频率低且访问频率高的数据，使用 Cache 来保存可以有效地提高网站的性能。

最后，表 1-14 是对以上三种数据持久化方式的特性对比。

表 1-14 Cookie、Session 和 Cache 对比

	Cookie	Session	Cache
存储位置	客户端	服务器	服务器
是否会被主动丢弃	不会	不会	会
与会话相关	是	是	否
是否被序列化	是	否	否
是否发生服务器-客户端传输	是	否	否
是否被加密	是	否	否

5．浏览器

浏览器是指可以显示网页服务器或者文件系统的HTML文件内容，并让用户与这些文件交互的一种软件，也就是在用户计算机上的万维网客户程序，其结构如图 1-113 所示。万维网文档所驻留的计算机则运行服务器程序，因此这个计算机也称为万维网服务器。客户程序向服务器程序发出请求，服务器程序向客户程序送回客户所要的万维网文档。在一个客户程序主窗口上显示出的万维网文档称为页面或网页。一个网页中可以包括多个文档，每个文档都是分别从服务器获取的。大部分的浏览器本身支持除了 HTML 之外的广泛的格式，例如 JPEG、PNG、GIF 等图像格式，并且能够扩展支持众多的插件（plug-ins）。另外，许多浏览器还支持其他的 URL 类型及其相应的协议，如FTP、Gopher、HTTPS（HTTP 协议的加密版本）。HTTP 内容类型和 URL 协议规范允许网页设计者在网页中嵌入图像、动画、视频、声音、流媒体等。

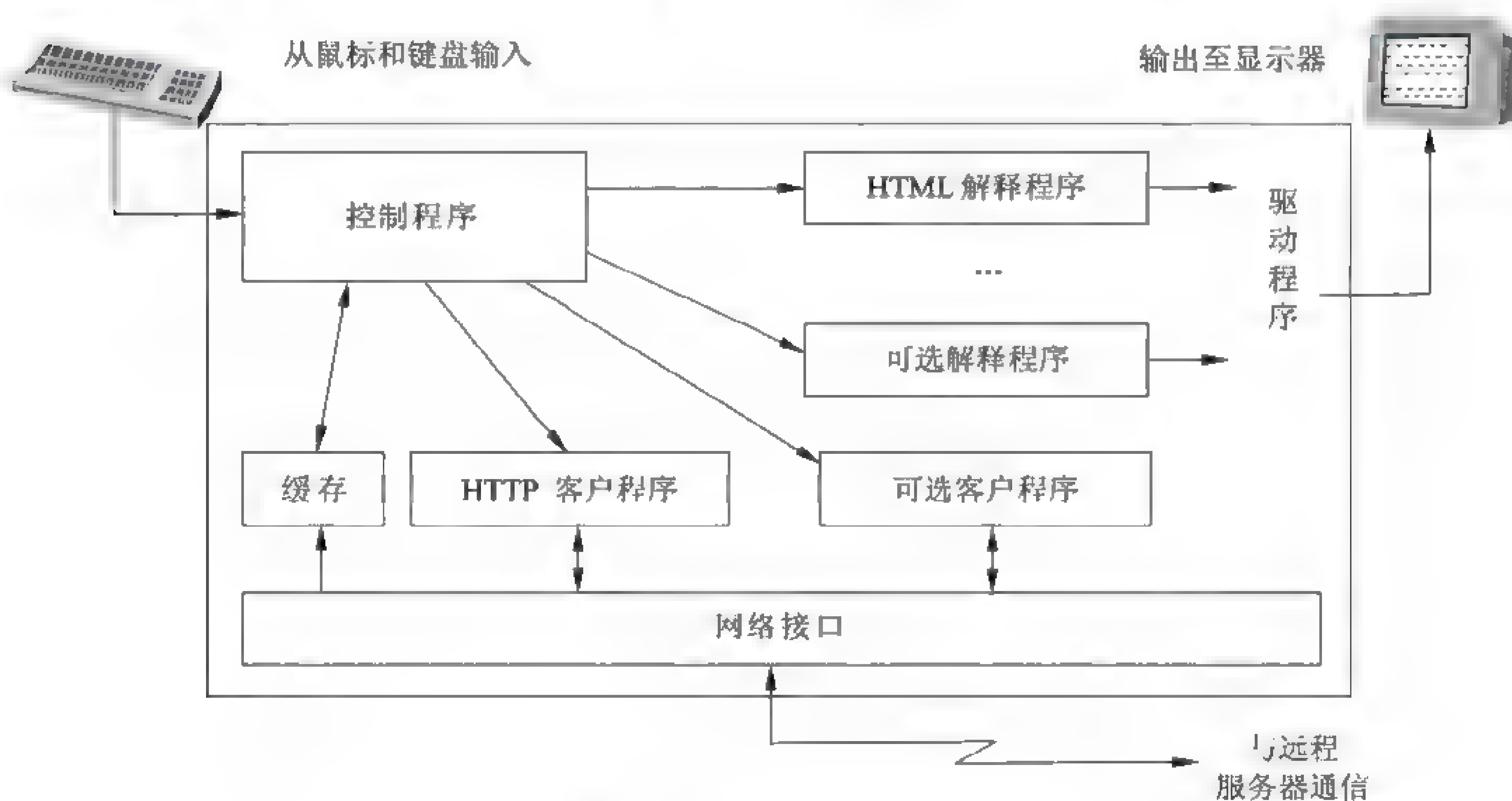


图 1-113　浏览器的结构

1.8.3.6　动态主机配置协议

1．DHCP 的功能

动态主机配置协议（DHCP）是一种使网络管理员能够集中管理和自动分配 IP 网络地址的通信协议。在 IP 网络中，每个连接 Internet 的设备都需要分配唯一的 IP 地址。DHCP 使网络管理员能从中心节点监控和分配 IP 地址。当某台计算机移到网络中的其他位置时，能自动收到新的 IP 地址。

DHCP 使用了租约的概念，或称为计算机 IP 地址的有效期。租用时间是不定的，主要取决于用户在某地连接 Internet 需要多久，这对于教育行业和其他用户频繁改变的

环境是很实用的。通过较短的租期，DHCP 能够在一个计算机比可用 IP 地址多的环境中动态地重新配置网络。同时，DHCP 也支持为计算机分配静态地址，如需要永久性 IP 地址的 Web 服务器。

2．DHCP 报文格式

DHCP 的报文格式如图 1-114 示。

8bits	8bits	8bits	8bits
Op	Htype	Hlen	Hops
Xid			
Secs		Flags	
Ciaddr			
Yiaddr			
Siaddr			
Giaddr			
Chaddr（16 bytes）			
Sname（64 bytes）			
File（128 bytes）			
Option（variable）			

图 1-114　DHCP 报文格式

- Op：消息操作代码，既可以是引导请求（BOOTREQUEST）也可以是引导答复（BOOTREPLY）。
- Htype：硬件地址类型。
- Hlen：硬件地址长度。
- Xid：处理 ID。
- Secs：客户机地址获取，进程恢复消耗的时刻。
- Flags：标记。
- Ciaddr：客户机 IP 地址。
- Yiaddr：“你的”（客户机）IP 地址。
- Siaddr：在 bootstrap 中使用的下一台服务器的 IP 地址。
- Giaddr：用于导入的接替代理 IP 地址。
- Chaddr：客户机硬件。
- Sname：任意服务器主机名称，空终止符。
- File：DHCP 发现协议中的引导文件名、空终止符、属名或者空，DHCP 供应协议中的受限目录路径名。
- Options：可选参数字段。参考定义选择列表中的选择文件。

3. DHCP 消息类型

DHCP 的消息类型如表 1-15 所示。

表 1-15　DHCP 消息类型

消　息	功　能
DHCPDISCOVER	客户进行广播以确定本地可用的服务器
DHCPOFFER	服务器给客户的应答，在其中包括了配置参数
DHCPREQUEST	此消息是客户发送给服务器的，作用有三个：客户从一台服务器上请求配置信息（在这个时候客户也就拒绝了其他服务器发来的地址，客户就用这个地址了）；在系统重新启动后，客户利用这个消息确认原来分配的网络地址仍然有效；客户还可以利用这个消息对特定的网络地址租用时间要求延期
DHCPACK	服务器发向用户的消息，包括了配置参数和网络地址
DHCPNAK	服务器发向用户的消息，告知客户当前使用的网络地址无效或租期已满
DHCPDECLINE	客户发向服务器的消息，告知服务器此地址已被使用
DHCPRELEASE	客户发向服务器的消息，告知服务器此地址不再使用
DHCPINFORM	客户发向服务器的消息，要求服务器发送本地配置信息，客户已经配置好了网络地址，不需要再发送网络地址了

4. DHCP 的工作过程

DHCP 采用客户服务器的工作方式。具体工作过程如下：

① DHCP 服务器打开 UDP 67 端口，监听请求。

② DHCP 客户从端口 68 利用 UDP 向服务器发送 DHCPDISCOVER 报文。

③ DHCP 服务器发送 DHCPOFFER 报文（凡收到 DHCP 发现报文的 DHCP 服务器都发出 DHCP 提供报文）。

④ DHCP 客户从多个 DHCP 服务器中选择一个，然后向其发送 DHCPREQUEST 报文。

⑤ DHCP 服务器回送 DHCPACK，包含分配的 IP 地址。

⑥ 租用期过了一半，DHCP 客户发送请求报文 DHCPREQUEST 要求更新租用期。

⑦ DHCP 服务器若同意，则发回确认报文 DHCPACK。DHCP 客户得到了新的租用期，重新设置计时器。

⑧ DHCP 服务器若不同意，则发回否认报文 DHCPNACK。这时 DHCP 客户必须立即停止使用原来的 IP 地址，而必须重新申请 IP 地址（回到步骤②）。

⑨ DHCP 客户可随时提前终止服务器所提供的租用期，这时只需向 DHCP 服务器发送释放报文 DHCPRELEASE 即可。

另外，若 DHCP 服务器不响应步骤⑥的请求报文 DHCPREQUEST，则在租用期过了 87.5% 时，DHCP 客户必须重新发送请求报文 DHCPREQUEST（重复步骤⑥），然后又继续后面的步骤。

1.8.3.7 无线 Web 协议（WAP）

1．WAP 的特点

① WAP 只要求移动电话和 WAP 代理服务器的支持，而不要求现有的移动通信网络协议作任何的改动，所以 WAP 能同时适用于 CDMA、DETC、GSM、IMT-2000 等多种不同的移动通信系统。

② WAP 协议堆栈的设计力求使所需带宽最小化，并对各种网络技术和服务提供广泛支持。

③ WAP 层次结构比较松散，每层的开发独立于其他层，容易引入新的传输协议和服务类型。

2．WAP 协议栈的组成结构

（1）应用层即无线应用环境（Wireless Application Environment，WAE），是基于 WWW 和移动电话技术而建立的一种通用应用环境，其协议栈如图 1-115 所示。WAE 提供了一个微浏览器，包含有下列功能：

- 解释并执行使用 WML 语言编辑的 WAP 网页。
- 包含 WML 脚本即 WMLScript，并能解释和执行采用该脚本语言编写的网页。
- 支持无线电话技术应用，包括电话技术服务 WTA 及其程序设计界面 WTAI。
- 定义了一组明确的数据格式，包括图像、电话本记录和日期信息等的数据格式。



图 1-115 WAP 协议栈

（2）无线会话层。无线会话层协议（Wireless Session Protocol，WSP）向两个对话服务提供一致接口的 WAP 应用层。一个是在 WTP 层上操作的连接导向服务，另一个是在安全或非安全数据包服务上操作的非连接服务 WDP。无线会话协议当前由与浏览应用相匹配的服务组成，通常简记为 WSP/B，它提供下列几项功能：

- 支持在压缩的超空间编码中的 HTTP/1 的功能和语义。
- 支持长久对话状态，以及通过对话移动暂停和恢复。

- 支持可靠或不可靠数据的普通设备的连接与访问。
- 支持协议特性流通。由于 WSP 体系的协议需要较长的反应时间，所以对低带宽载体网络的应用进行了优化，从而使 WSP/B 设计得允许 WAE 代理把 WSP/B 客户连接到 HTTP 服务器。

（3）传输协议层。无线传输协议层（Wireless Transaction Protocol，WTP）在数据包服务的顶端运行，并提供适合在“瘦”客户即移动网络站上执行的普通事务服务，并可对移动终端进行优化，主要提供以下功能。

- 三个级别的传输服务：不可靠单向请求、可靠单向请求、可靠双向请求与答复。
- 用户对收到信息的确认。
- 对超频带数据的确认。
- 旨在减少传送信息数量的 PDU 串联延迟。
- 异步传输服务。

（4）安全协议层。无线传输安全层协议（Wireless Transport Layer Security，WTLS）是基于工业标准传输层安全协议的协议，它在安全传输协议 SSL 的基础上针对 WAP 传输所用的低带宽通信信道进行了优化，主要为数据传递提供下列功能和服务。

- 保证数据在终端和应用服务器间稳定、准确地传送。
- 保证数据在终端和应用服务器间传输的保密性，避免数据传输中的截取、窃听。
- 保证终端应用服务器的真实性。
- 对不能顺利通过核对的数据进行检测，如果必要则驳回数据，使对方重新发送。
- 保证终端之间的通信安全。

（5）数据报协议层。无线数据报协议（Wireless Datagram Protocol，WDP）用于传输数据，发送和接收消息。它可以向 WAP 的上层协议提供服务支持，并保持通信的透明性，同时能够独立运行下部无线网络。在保持传输接口和基本特性一致的情况下，WDP 采用中间网关可以实现全局工作的互用性，从而实现无线数据的顺利传输。

3. WAP 工作原理

为适应无线设备屏幕小、无线传输带宽小等环境的特殊要求，WAP 采取了以下措施：

① 使用二进制传输经过高度压缩的数据，并对长延时和中低带宽进行优化。

② WAP 的会话功能可以处理不连续覆盖的问题，并能自动地在 IP 不可用时改用其他优化协议来进行各种信息传输。

③ 通过使用 WML 语言编写网页，WAP 解决了 Internet 页面不能在移动通信设备上显示的问题。

④ 运用 WML 编辑的网页可在手机的微浏览器上产生按钮、图示及超链接等功能，并可提供信息浏览、数据输入、文本和图像显示、表格显示等功能，大大减小了在移动设备上浏览网页内容的复杂程度。

⑤ WAP 通过加强网络功能来弥补便携式移动设备本身的缺陷，工作时尽可能少地

占用移动通信设备的资源。

⑥ WAP 在应用层上隐藏了 GSM 的复杂性，给用户提供了类似于普通 Web 页面的友好性。

⑦ WAP 通过使用类似于 JavaScript 的脚本语言 WMLScript，来使移动通信设备先将信息进行处理后再发给服务器。

1.8.3.8 P2P 应用协议

1．概述

对等连接 P2P 是 peer-to-peer 的缩写，P2P 也就可以理解为“伙伴对伙伴”的意思，或称为对等连接。目前人们认为其在加强网络上人的交流、文件交换、分布计算等方面大有前途。简单地说，以前人们下载文件是从服务器上，而 P2P 则是多个终端用户各下载一部分，然后互相下载，这样大量用户同时下载不但不会造成堵塞，反而速度加快。

简单的说，P2P 直接将人们联系起来，让人们通过互联网直接交互。P2P 使得网络上的沟通变得容易，共享和交互更直接，真正地消除中间商。 P2P 就是人可以直接连接到其他用户的计算机，交换文件，而不是像过去那样连接到服务器去浏览与下载。 P2P 另一个重要特点是改变互联网现在的以大网站为中心的状态，重返“非中心化”，并把权力交还给用户。

2．P2P 的发展过程

P2P 的发展可以被划分为三代。

（1）第一代是以 Napster 为代表的，还用中央服务器管理的 P2P，这一代的 P2P 生命力十分脆弱：只要关闭服务器，网络就死了。

（2）第二代分布式 P2P 没有中央服务器，但是速度太慢。

（3）第三代为混合型，采用分布服务器。目前我国流行的 BT 下载和电驴就是属于这类。

3．P2P 工作过程

使用者首先一定要下载而且运行一个点到点连网程序。在开始程序之后，使用者进入属于网络的另外一部计算机的 IP 地址。（典型地，使用者下载的网页将会把一些 IP 地址列为开始位置） 一经计算机寻找的另外的一个网络成员在线，它将会连接到那个使用者。使用者能选择一次连接多少成员，而且决定他们愿意共享哪一个文件，还可以用密码保护。

4．P2P 的优势

- 非中心分散化：将以服务器为中心的服务分散到各个网络节点，避免出现服务器性能瓶颈。
- 扩展性：随着更多的用户加入，网络整体资源和服务得到了提升和扩充。
- 健壮稳定性：网络自组织管理，网络中某一节点或局部网络出现问题对整个网络不会有很大的影响。

- 资源共享：能有效的利用网络中闲置的硬件资源进行计算、存储。
- 优化传播速度：数据传播是直接在节点之间传送的，因此当用户数据增加时，其数据传播速度会大大加强。

1.8.4　代理与 NAT

1．应用层代理

代理（Proxy）处于客户机与服务器之间，对于服务器来说，Proxy 是客户机，Proxy 提出请求，服务器响应；对于客户机来说，Proxy 是服务器，它接受客户机的请求，并将服务器上传来的数据转给客户机。

应用层代理工作在 TCP/IP 模型的应用层之上，它只能用于支持代理的应用层协议（如 HTTP、FTP）。

应用层代理的原理是彻底隔断通信两端的直接通信，所有通信都必须经应用层代理层转发，访问者任何时候都不能与服务器建立直接的 TCP 连接，应用层的协议会话过程必须符合代理的安全策略要求。

代理服务器实现模型如图 1-116 所示。

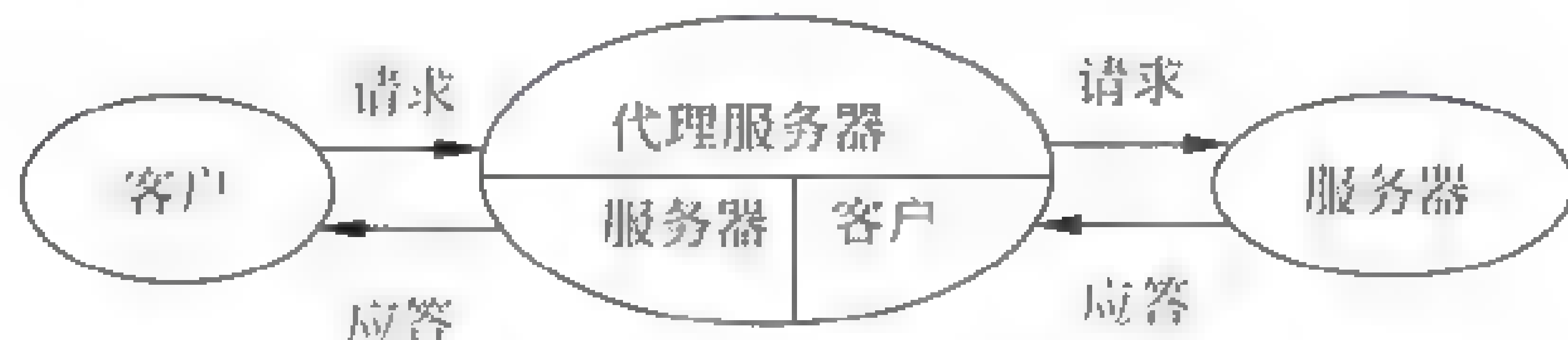


图 1-116　代理服务器实现模型图

2．网络地址转换（NAT）

因特网的 IP 地址有本地地址和全球地址两类。本地地址仅在机构内部使用，由本机构自行分配，而不需要向因特网的管理机构申请。全球地址顾名思义在全球唯一，必须向因特网的管理机构申请。 由于本地地址可以由机构自行分配，在一定程度上缓解了 IP 地址不足的问题。RFC1918 为私有和内部使用的网络留出了三个 IP 地址块（A 类、B 类和 C 类地址范围各一段）作为专用地址，也就是本地地址。但因特网中的所有路由器对目的地址是专用地址的数据报一律不进行转发。这就需要使用网络地址转换（Network Address Translation，NAT）。通常由路由器担任 IP 转换的功能，且要在专用网连接到因特网的路由器上安装 NAT 软件，装有 NAT 软件的路由器叫做 NAT 路由器，它至少有一个有效的外部全球地址。

NAT 有三种类型：静态 NAT、动态地址 NAT、端口地址转换 PAT。

- 静态 NAT：设置起来最为简单和容易，内部网络中的每个主机都被永久映射成某个全球地址。
- 动态地址 NAT：以地址池的方式。地址池中有多个全球地址用来对内部地址进行

映射，但不固定绑定。

- 端口地址转换 PAT：一个外网地址可以和多个内网地址（如一个网段）进行映射，同时在该地址上加上一个由 NAT 设备指定的 TCP/UDP 的端口号来进行区分。通过使用 PAT 可以让成百上千的本地地址节点使用一个全球地址访问 Internet。PAT 普遍应用于接入设备中，它可以将中小型的网络隐藏在一个合法的 IP 地址后面。通过这种方式把内部主机隐藏起来，从而实现了内部主机的安全性。

1.8.5 搜索引擎

搜索引擎（search engine）是指因特网上专门提供查询服务的一类网站，这些网站通过网络搜索软件（又称为网络搜索机器人）或网站登录等方式，收集因特网上大量网站的页面，经过加工处理后建库，从而能够对用户提出的各种查询做出响应，提供用户所需的信息。它是一个对互联网资源进行搜索整理和分类，并储存在网络数据库中供用户查询的系统，包括信息搜索、信息分类、用户查询三部分。

1．搜索引擎的工作原理

简单的说，搜索引擎是通过从互联网上提取的各个网站的信息来建立数据库，检索与用户查询条件匹配的相关记录，然后按一定的排列顺序将结果返回给用户。根据搜索引擎提取数据的方法，可将搜索引擎系统分为三大类。

1）目录式搜索引擎

目录式搜索引擎是一种网站级搜索引擎。目录式搜索引擎由分类专家将网络信息按照主题分成若干个大类，每个大类再分为若干个小类，依次细分。一般的搜索引擎分类体系有五六层，有的甚至十几层。先由程序自动搜集信息，然后由编辑员查看信息，人工形成信息摘要，提供目录浏览服务和直接检索服务。由于目录式搜索引擎的信息分类和信息搜集有人的参与，因此其搜索的准确度是相当高的。缺点是需要人工介入、维护量大、信息量少、信息更新不够及时。Yahoo 属于这类搜索引擎。

2）机器人搜索引擎

这种搜索方式是搜索引擎主动派出称为蜘蛛（spider）的机器人程序定期搜索，对一定 IP 地址范围内的互联网站进行检索，一旦发现新的网站，它会自动提取网站的信息和网址加入自己的数据库。该类搜索引擎的优点是信息量大、更新及时、毋需人工干预。缺点是返回信息过多、有很多无关信息、用户必须从结果中进行筛选。Google、百度属于这类搜索引擎。

3）元搜索引擎

这类搜索引擎没有自己的数据，而是将用户的查询请求同时向多个预先选定的独立搜索引擎递交，将返回的结果进行重复排除、重新排序等处理后，作为自己的结果返回给用户。优点是返回结果的信息量更大、更全。缺点是用户需要做更多的筛选。

2．搜索引擎的性能指标

1973 年美国的 Lancaster 和 Fayen 曾列出 6 项衡量信息检索系统效果的评价指标，

即覆盖范围、查全率、查准率、响应时间、用户负担和检索结果输出格式。中文搜索引擎的评价标准主要有：收录范围、查询结果反馈信息的质量、检索款式目的信息量、查错率、更新与报道速度、查询功能、检索界面的友好性、精品推荐、友情链接、响应速度。

搜索引擎的目标就是在非常短的时间内搜索的信息全面并且准确。传统信息检索系统的性能参数召回率和精度同样也可以衡量一个搜索引擎的性能。召回率是检索出的相关文档数和文档库中所有的相关文档数的比率，衡量的是搜索引擎的查全率；精度是检索出的相关文档数与检索出的文档总数的比率，衡量的是搜索引擎的查准率。对于一个检索系统来讲，召回率和精度不可能两全其美。召回率高时，精度低；精度高时，召回率低。因为没有一个搜索引擎系统能够搜集到所有的 NDC 网页所以召回率很难计算。

1.9　网络管理

1.9.1　网络管理基本概念

1．计算机网络定义

网络管理是指对网络的运行状态进行检测和控制，并能提供有效、可靠、安全、经济地服务。网络管理应完成两个任务，一是对网络的运行状态进行监测，二是对网络的运行状态进行控制。通过监测可以了解当前网络状态是否正常，是否出现危机和故障；通过控制可以对网络状态进行合理分配，提供网络性能，保证网络应有的服务。监测是控制的前提，控制是监测的结果。所以，网络管理就是对网络的监测和控制。

2．网络管理模型

在网络管理中，一般采用管理站-代理的管理模型，如图 1-117 所示，它类似于客户机/服务器模式，通过管理进程与一个远程系统相互作用实现对远程资源的控制。在这种简单的体系结构中，一个系统中的管理进程担当管理站角色，被称为网络管理站，而另一个系统中的对等实体担当代理者角色，被称为管理代理。网络管理站将管理要求通过管理操作指令传送给位于被管理系统中的管理代理，对网络内的各种设备、设施和资源实施监视和控制，管理代理则负责管理指令的执行，并且以通知的形式向网络管理站报告被管对象发生的一些重要事件。

1）网络管理站

网络管理站（network manager）一般位于网络系统的主干或接近主干位置的工作站、微机等，负责发出管理操作的指令，并接收来自代理的信息。网络管理站要求管理代理定期收集重要的设备信息。网络管理站应该定期查询管理代理收集到的有关主机运行状态、配置及性能数据等信息，这些信息将被用来确定独立的网络设备、部分网络或整个网络运行的状态是否正常。

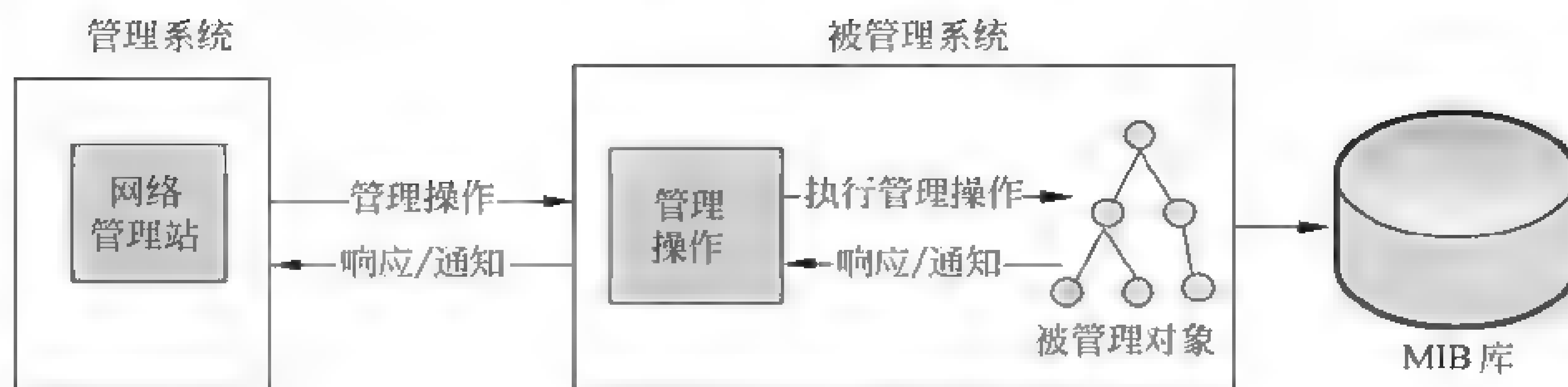


图 1-117 管理站-代理模型

网络管理站和管理代理通过交换管理信息来进行工作，信息分别驻留在被管设备和管理工作站上的管理信息库中。这种信息交换通过一种网络管理协议来实现，具体的交换过程是通过协议数据单元（PDU）进行的。通常是管理站向管理代理发送请求 PDU，管理代理以响应 PDU 回答，管理信息包含在 PDU 参数中。在有些情况下，管理代理也可以向管理站发送通知，管理站可根据报告的内容决定是否做出回答。

2）管理代理

管理代理（network agent）则位于被管理的设备内部。通常将主机和网络互连设备等所有被管理的网络设备称为被管设备。管理代理把来自网络管理站的命令或信息请求转换为本设备特有的指令，完成网络管理站的指示，或返回它所在设备的信息。网络代理也可能因为某种原因拒绝网络管理站的指令。另外，管理代理也可以把在自身系统中发生的事件主动通知给网络管理站。

3）网络管理协议

用于网络管理站和管理代理之间传递信息，并完成信息交换安全控制的通信规约就称为网络管理协议。网络管理站通过网络管理协议从管理代理那里获取管理信息或向管理代理发送命令；管理代理也可以通过网络管理协议主动报告紧急信息。

目前最有影响的网络管理协议是 SNMP 和 CMIS/CMIP，它们代表了目前两大网络管理解决方案。其中 SNMP 流传最广，应用最多，获得支持也最广泛，已经成为事实上的工业标准。

4）管理信息库

管理信息库（Management Information Base，MIB）是一个信息存储库，是对于通过网络管理协议可以访问信息的精确定义，所有相关的被管对象的网络信息都放在 MIB 上。MIB 库的描述采用了结构化的管理信息定义，称为管理信息结构（Structure of Management Information，SMI），它规定了如何识别管理对象以及如何组织管理对象的信息结构。MIB 库中的对象按层次进行分类和命名，整体表示为一种树型结构，所有被管对象都位于树的叶子节点，中间节点为该节点下的对象的组合。

3．网络管理功能

为了标准化系统的管理功能，ISO 在 ISO/IEC 7498-4 文档中定义了网络管理的 5 个

系统管理功能域（SMFA），即配置管理、故障管理、性能管理、计费管理和安全管理。

1）配置管理

配置管理负责网络的建立、业务的开展以及配置数据的维护。配置管理的作用包括确定设备的地理位置、名称和有关细节，记录并维护设备参数表；用适当的软件设置参数值并配置设备功能；初始化、启动和关闭网络及其相应设备；维护、增加和更新网络设备以及调整网络设备之间的关系。配置管理对资源的管理信息库（MIB）建立资源数据，并对其进行维护。配置管理可以根据网络管理人员的命令自动调整网络设备配置，以保证整个网络性能达到最优。

2）故障管理

故障管理的主要是及时发现和排除网络故障，其目的是保证网络能够提供连续、可靠、优质的服务。故障管理用于保证网络资源无障碍无错误的运营状态，它包括障碍管理、故障恢复和预防保障。障碍管理的内容有警告、测试、诊断、业务恢复和故障设备更换等在系统可靠性下降，业务经常受到影响时，预防保障为网络提供治愈能力。如果设备状态发生变化或者发生故障的设备被替换，则要与资源 MIB 互通，以尽快修改 MIB 中的信息。

3）性能管理

性能管理的目的是维护网络服务质量（QoS）和网络运营效率。为此性能管理要提供性能监测功能、性能分析功能以及性能管理控制功能。同时，还要提供性能数据库的维护以及在发现性能严重下降时启动故障管理系统的功能。典型的网络性能管理可以分为性能监测和网络控制。其中性能监测是对网络工作状态信息的收集和整理；而网络控制则是为改善网络设备的性能而采取的动作和措施。

4）计费管理

计费管理的主要目的是正确地计算和收取用户使用网络服务的费用，同时，还要进行网络资源利用率的统计和网络的成本效益核算。其中，有账目记录、账单验证和费率折扣处理等。对于一个以赢利为目的的网络经营者来说，资费政策是很重要的，计费管理功能提供了对用户收费的依据。

5）安全管理

安全管理采用信息安全措施保护网络中的系统、数据和业务。安全管理与其他管理功能有着密切的关系。安全管理要调用配置管理中的系统服务对网络中的安全设施进行控制和维护。当网络发现有安全方面的故障时，要向故障管理通报安全故障事件以便进行故障诊断和恢复。

安全管理功能还要接收计费管理发来的与访问权限有关的计费数据和访问事件通报。安全管理的目的是提供信息的隐私、认证和完整性保护机制，使网络中的服务、数据以及系统免受入侵者的侵扰和破坏。一般的安全管理系统包含风险分析功能、安全服务功能、警告、日志和报告功能以及网络管理系统保护功能等。

4．网络管理系统组成

网络管理系统（NMS）是网络监视和控制工具的集合，一般包含以下一些观点：

（1） 为执行大多数或全部的管理任务，有一个单一操作接口，这个接口拥有功能强大且用户界面友好的命令集。

（2）使用最少数量的专用设备。也就是说，网络管理所需要的大多数软件和硬件都被组合到现有的用户设备中。

网络管理系统由现有网络组件中所添加的硬件和软件组成。执行网络管理任务的软件存在于主机或者设备中（如前端处理器、终端控制器、网桥、路由器）。网络管理系统把整个网络看做一个统一结构来处理，每个节点都有系统所知的地址、标签和每个元素的具体属性。网络的节点定期反馈统计信息到网络管理系统。

网络管理系统应该能够实现网络的故障管理、网络流量控制、计费功能、网络的安全功能以及网络路由选择策略管理等功能。

网络管理系统底层需要支持管理协议，比如SNMP，负责与SNMP实体通信以达到监控目的。上层需要具有用户接口，接收用户命令，并统计、分析、日志等相关功能。

5．网络管理与系统管理

网络管理是确保网络用户获得信息技术服务及所期望的服务质量。为了实现这个目标，管理需要建立策略与用户建立正规的服务质量认可协议。从商业管理的角度来看，网络管理涉及网络工程部、运营部和维护部的战略性和战略规划，以及当前和将来所需服务的最小成本。

当一个用户从各自的工作站通过客户端不能访问服务器应用程序时，这可以归因于应用程序故障，或者归因于从客户的工作站到服务器操作平台的传输故障。前者属于系统故障，应该归入系统管理。后者属于连接故障，应该归入网络的故障管理。系统管理归纳为在网络中的系统及系统资源管理。网络管理负责网络资源（如集线器、交换机、网桥、路由器和网关），以及它们通过网络的相互连通性。网络管理也处理网络中任意两个处理机间端对端的连接。

6．网络管理标准

为了支持各种网络的互连及其管理，网络管理需要有一个国际性的标准。在众多的标准化组织中，目前国际上公认最著名、最具有权威的是国际标准化组织ISO和国际电信联盟的电信标准部ITU-T（即原来的国际电报电话咨询委员会CCITT），而计算机网络中，IETF的因特网技术标准已成为实事上的国际标准。

1）ISO

国际标准化组织（ISO）成立于1947年，是世界上最庞大的一个国际性标准化专门机构，也是联合国的甲级咨询机构。它的会址在日内瓦。我国1947年就加入了ISO。

ISO的成员分为P成员和O成员，P（participation）成员有表决权，而O（observer）成员不参加ISO的技术工作，只是与ISO保持密切联系。

ISO 的技术工作由技术委员会（Technical Committee，TC）具体负责，每个 TC 可以成立分技术委员会 SC（subcommittee）或工作组（Work Group，WG），其成员是各国的专家。

网络管理标准是由 ISO 的第 97 委员会（即信息处理系统技术委员会）下的第 21 分委员会中的第 4 工作组制定的。通常记为 ISO/TC97/SC21/WG4。

ISO 每个标准的制定过程要经历下面的 5 个步骤：

（1）每个技术委员会根据其工作范围拟定相应的工作计划，并报理事会下属的计划委员会批准。

（2）相应的分技术委员会的工作组根据计划编写原始工作文件，称为工作草案。

（3）分技术委员会或工作组再把工作草案提交技术委员会或分技术委员会作为待讨论的标准建议，称委员会草案（Committee Draft，CD），而 ISO 则要给每个 CD 分配一个唯一的编号，相应的文件被标记为 ISO CDxxxx。委员会草案 CD 之间的文件叫做建议草案（Draft Proposal，DP）。

（4）技术委员会将委员会草案发给其成员征求意见。若 CD 得到大多数 P 成员的同意，则委员会草案 CD 就成为国际标准草案（Draft International Standard，DIS），其编号不变。

（5）ISO 的中央秘书处将 DIS 分别送给 ISO 的所有成员国投票表决。有 75%的成员国赞成则通过。经 ISO 的理事会批准以后就成为正式的国际标准（International Standard，IS），其编号不变，标记为 ISOxxxx。

ISO 还有一些被称为技术报告（Technical Report，TR）的非标准文件。这些文件不需要提交相应委员会通过。TR 是技术委员会再制定标准过程中形成的一些中间结果，可以给 TR 进行编号，标记为 ISO TRxxxx。

当各阶段的标准文件需要补充修改时，ISO 在相应标准文件的后面增加一个补篇（AMendment，AM）。补篇前面冠以标准的名称，如委员会草案补篇 CDAM。

ISO 规定每 5 年对国际标准进行一次复审，过时的标准将被废除。

ISO 对网络管理的标准化始于 1979 年，目前已经产生了一部分国际标准。尽管 ISO 的网络管理标准因为过于复杂而迟迟得不到广泛的应用，但其他一些国际性、专业性或区域性的标准化组织还是经常采用 ISO 的网络管理标准作为他们自己参考标准，有时只是换一个编号而已。

2）ITU-T

国际电信联盟（International Telecommunication Union，ITU）成立于 1934 年，是联合国下属的 15 个专门机构之一。ITU 在 1989 年下设 5 个常设机构，它们分别是秘书处、国际电报电话咨询委员会（Consultative Committee on International Telegraph and Telephone，CCITT）、国际无线电咨询委员会（Consultative Committee of International

Radio，CCIR)、国际频率登记委员会（International Frequency Registration Board，IFRB）改为无线电通信部门（Radicommunication Sector，RS）和电信发展局（Bureau of Development of Telecommunication，BDT)。

CCITT 和 CCIR 的主要任务是研究电报、电话和无线电通信的技术标准以及业务、资费和发展通信网技术的经济问题。为国际电联制定各种规则提供技术业务依据。

随着技术的进步，有限和无线已进行了融合。从 1993 年起，国际电联将 CCITT 和 CCIR 合并，成立一个新的电信标准化部门（Telecommunication Standardization Sector，TSS)。而原来的国际频率登记委员会 IFRB 改为无线电通信部门 RS，原来的 BDT 改为电信发展部门（Telecommunication Development Sector，TDS)。此后国际电联有关电信的国际标准（仍称为建议书）均由电信标准化部门 TSS 制定。国际电联规定，电信标准化部门的简称为 ITU-T。

虽然 CCITT 和 CCIR 不复存在，但它们以前发行的建议书仍然有效。在应用原 CCITT 制定的标准时，可按原来的写法，如 CCITT X.25，但最好还是采用新的写法 ITU-T X.25。

ITU-T 的标准化工作由其设立的研究组（Study Group，SG）进行。其中与网络管理有关的研究组有以下 4 个：

- SG2 网络运行（network operation)。有关电信业务定义的一般问题该组进行电信网络的管理和网络的服务质量的研究工作。
- SG4 网络维护（network maintenance)。负责电信管理网络（TMN）的研究；有关网络及其组成部分的维护，确立所属的维护机制；由其他研究组提供的专门维护机制的应用。
- SG7 数据网和开放系统通信（data networks and open systems communication)。该组负责系统互连中的管理标准研究。
- SG11 交换和信令（switching and signalling)。该组负责电信管理网的研究工作。

原 CCITT 已经用 X.700 系列制定了一系列管理标准（建议书），这些标准和 ISO 的网络管理标准基本上相同，只是采用了各自的编号体系。而 ITU-T 的网络管理标准（建议书）中最著名的是有关电信管理网 TMN 的 M 系列建议书。

3）IETF

Internet 体系结构委员会 IAB 是 1992 年从 Internet 活动委员会改名而来，它是 Internet 协议的开发和一般体系结构的权威控制机构。SNMP 的标准及其演变都是在 Internet 体系结构委员会的引导下由 IETF 制定和发布的。

IAB 下设的子机构称为任务组，共设两个。它们的时间表和任务各不相同，分别是 Internet 研究任务组（IRTF）和 Internet 工程任务组（IETF)，相应由 Internet 研究指导组（IRSG）和 Internet 工程研究组（IERG）领导。图 1-118 给出了它们之间的关系。IRTF 主要致力于长期研究与开发，而 IETF 则注重于相对短期的工程项目。

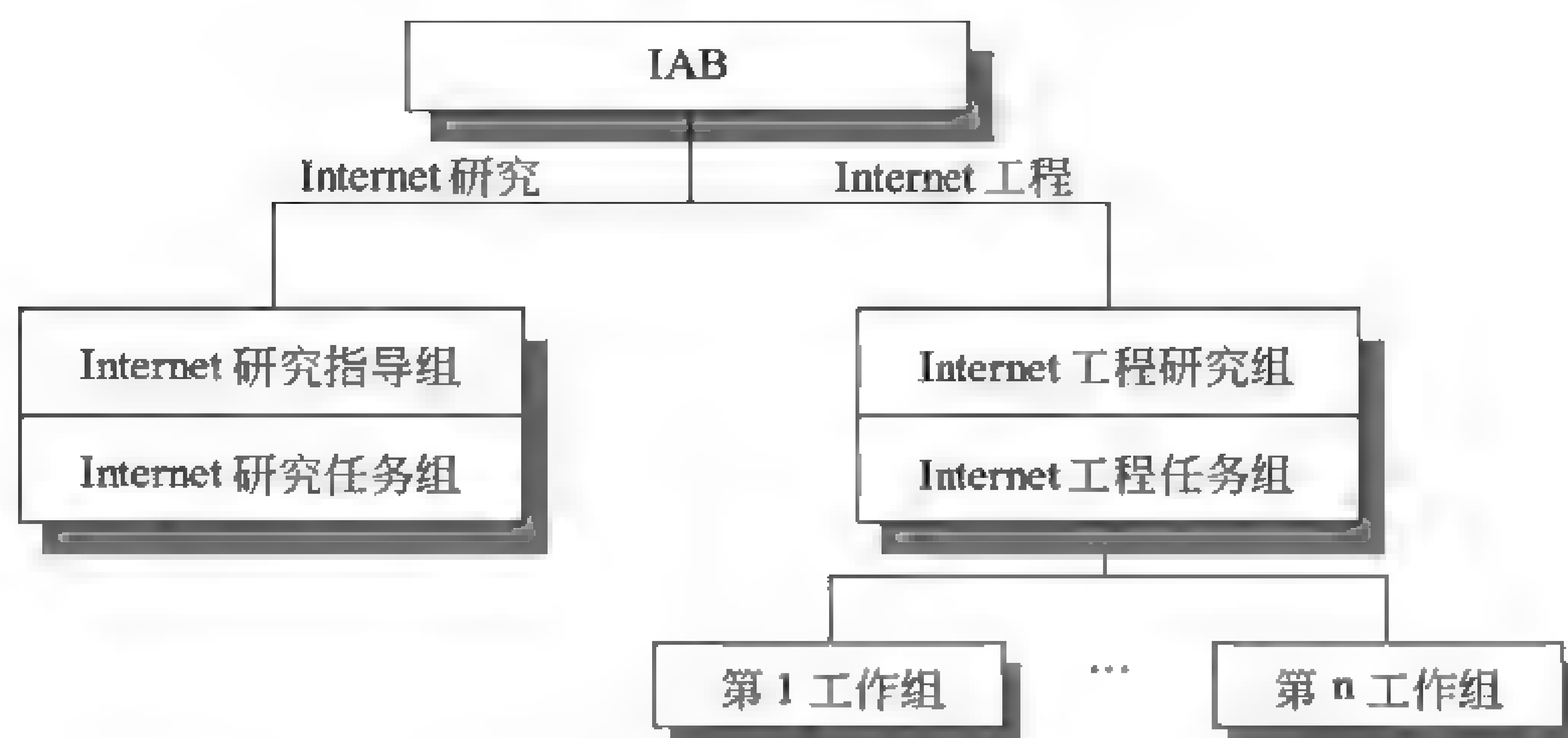


图 1-118　Internet 体系结构委员会 IAB 的机构组织

为了更有效的工作，IETF 按地区分成多个工作组（WG）。每个工作组都有自己具体的工作目标，通常每年开三次会。工作组是由对请求注解（Request For Comments，RFC）文档的形成有技术性贡献的人员组成，他们都是为制定 RFC 做研究工作。一旦工作完成，相关的工作组就会解散，他们的工作成果通常以 RFC 的形式公布于众。IESG 由每个地区工作组的负责人和 IETF 主席组成，这些负责人称为地区主任。

SNMP 各标准阶段的规范都是用 RFC 发布的。最早的 SNMP 工作组于 1991 年 11 月解散，而提出 SNMPv2C 的 RFC1901～1908 工作组也于 1995 年春解散。除了以 SNMP 标准为主要内容的工作组之外，许多新组纷纷成立，研究与 SNMP 有关的众多课题，其中为研究新的 MIB 组而成立的工作组就是最典型的代表。

4）其他组织

除了权威的国际性标准化组织以外，国际上还有一些民间团体和地区性机构也在进行有关网络管理标准化方面的研究。他们的结果对外界并没有约束力，只是作为团体的内部标准，对国际标准有一定的影响。

NMF（Network Management Forum）是由 120 多个公司组成的非官方标准化组织，该组织的成员主要由网络运营公司、计算机厂商、电信设备制造厂商、软件厂商、政府机构、系统集成商和银行等组成。NMF 的目标是针对互连信息系统中公共的、基于标准的管理办法的需求进行世界性的推广和实现。NMF 并不定义自己的标准，它只是在 ISO 和 ITU-T 的标准中定义功能选项，与任何国际性标准化团体都没有正式的联盟关系。NMF 的规范形成的文档集，称为 OMNIPoints（开放管理互操作性指南）。

1.9.2　管理信息的组织与表示

1.9.2.1　抽象语法表示 ASN.1

ASN.1 是由 CCITT 和 ISO 共同开发的正规语言，它与应用层一起使用，可在系统间进行数据的传输。作为一种形式语言，ASN.1 有严格的 BNF 定义。我们不想全面研究

它的 BNF 定义，而是自底向上地解释 ASN.1 基本概念，然后给出一个抽象数据类型的例子。下面列出 ASN.1 文本的书写规则，这些规则叫做文字约定（Lexical Conventions，LC）。

（1）书写的布局是无效的，多个空格和空行等效于一个空格。

（2）用于表示值和字段的标识符、类型指针（类型名）和模块名由大小写字母、数字和短线（hyphen）组成。

（3）标识符以小写字母开头。

（4）类型指针和模块名以大写字母开头。

（5）ASN.1 定义的内部类型全部用大写字母表示。

（6）关键字全部用大写字母表示。

（7）注释以一对短线（--）开始，以一对短线或行尾结束。

在 ASN.1 中，每一个数据类型都有一个标签（tag），标签有类型和值（见表 1-16）。数据类型是由标签的类型和值唯一决定的，这种机制在数据编码时有用。标签的类型分 4 种。

- 通用标签：用关键字 UNIVERSAL 表示。带有这种标签的数据类型是由标准定义的，适用于任何应用。
- 应用标签：用关键字 APPLICATION 表示，是由某个具体应用定义的类型。
- 上下文专用标签：这种标签在文本的一定范围（例如一个结构）中适用。
- 私有标签：用关键字 PRIVATE 表示，这是用户定义的标签。

表 1-16 ASN.1 定义的通用类型

标　签	类　型	值　集　合
UNIVERSAL1	BOOLEAN	TURE，FALSE
UNIVERSAL2	INTEGER	正数、负数和 0
UNIVERSAL3	BIT STRING	0 个或多个比特组成的序列
UNIVERSAL4	OCTET STRING	0 个或多个字节组成的序列
UNIVERSAL5	NULL	空类型
UNIVERSAL6	OBJECT IDENTIFIER	对象标识符
UNIVERSAL7	Object Descriptor	对象描述符
UNIVERSAL8	EXTERNAL	外部文件定义的类型
UNIVERSAL9	REAL	所有实数
UNIVERSAL10	ENUMERATED	整数值的表，每个整数有一个名字
UNIVERSAL11～15	保留	为 ISO 8824 保留
UNIVERSAL16	SEQUENCE，SEQUENCE OF	序列
UNIVERSAL17	SET，SET OF	集合
UNIVERSAL18	NumericString	数字 0～9 和空格
UNIVERSAL19	PrintableString	可打印字符串
UNIVERSAL20	TeletexString	由 CCITT T.61 建议定义的字符集

续表

标　签	类　型	值　集　合
UNIVERSAL21	VideotexString	由 CCITT T.100 和 T.101 建议定义的字符集
UNIVERSAL22	IA5String	国际标准字符集 5（相当于 ASCII 码）
UNIVERSAL23	UTCTime	时间
UNIVERSAL24	GeneralizedTime	时间
UNIVERSAL25	GraphicString	由 ISO 8824 定义的字符集
UNIVERSAL26	VisibleString	由 ISO 646 定义的字符集
UNIVERSAL27	GeneralString	通用字符集
UNIVERSAL28…	保留	为 ISO 8824 保留

ASN.1 定义的通用数据类型有 20 多种，标签值类型都是 UNIVERSAL，如表 1-16 所示。这些数据类型可分为四大类。

- 简单类型：由单一成分构成的原子类型。
- 构造类型：由两种以上成分构成的构造类型。
- 标签类型：由已知类型定义的新类型。
- 其他类型：包括 CHOICE 和 ANY 两种类型。

ASN.1 中的应用类型与特定的应用有关，根据网络管理的实际特点，SNMP 补充了一些特有的类型，RFC1155 定义了以下 6 种应用类型。

（1）NetworkAddress::=CHOICE{internet IpAddress}　这种类型用 ASN.1 的 CHOICE 构造定义，可以表示不同类型的网络地址。目前只有 Internet 地址，即 IP 地址。

（2）IpAddress::=[APPLICATION 0] IMPLICIT OCTET STRING（SIZE（4））　32 位的 IP 地址，定义为 OCTET STRING 类型。

（3）Counter::= [APPLICATION 1] IMPLICIT INTEGER（0..4294967295）　计算器类型是一个非负整数，其值可增加，但不能减少，达到最大值 $2^{32}-1$ 后回 0，再从 0 开始增加，计数器可用于计算收到的分组数或字节数。

（4）Gauge::=[APPLICATION 2] IMPLICIT INTEGER（0..4294967295）　计量器类型是一个非负整数，其值可增加，也可减少。计量器的最大值为 $2^{32}-1$。与计数器不同的地方是计量器达到最大值后不回 0，而是锁定在 $2^{32}-1$，直到复位，计量器可用于表示存储在缓冲队列中的分组数。

（5）TimeTicks::=[APPLICATION 3] IMPLICIT INTEGER（0..4294967295）　时钟类型是非负整数。计数范围 $1\sim2^{32}-1$，以 0.01s 为单位递增，可表示从某个事件（例如设备启动）开始到目前经过的时间。

（6）Opaque::=[APPLICATION 4] OCTET STRING　不透明类型即未知数据类型，它可以表示任意类型。这种数据编码时按 OCTET STRING 处理，管理站和代理能解释这种类型。

1.9.2.2　基本编码规则

BER码有三个字段：标签（tag）字段是关于标签类别和编码格式的信息；长度（length）字段定义内容字段的长度；值（value）字段包含实际的数据。因此，一个BER编码实际是一个TLV三元组（标签，长度，值）。每个字段都是一个或多个8位位组组成，结构如图1-119所示。

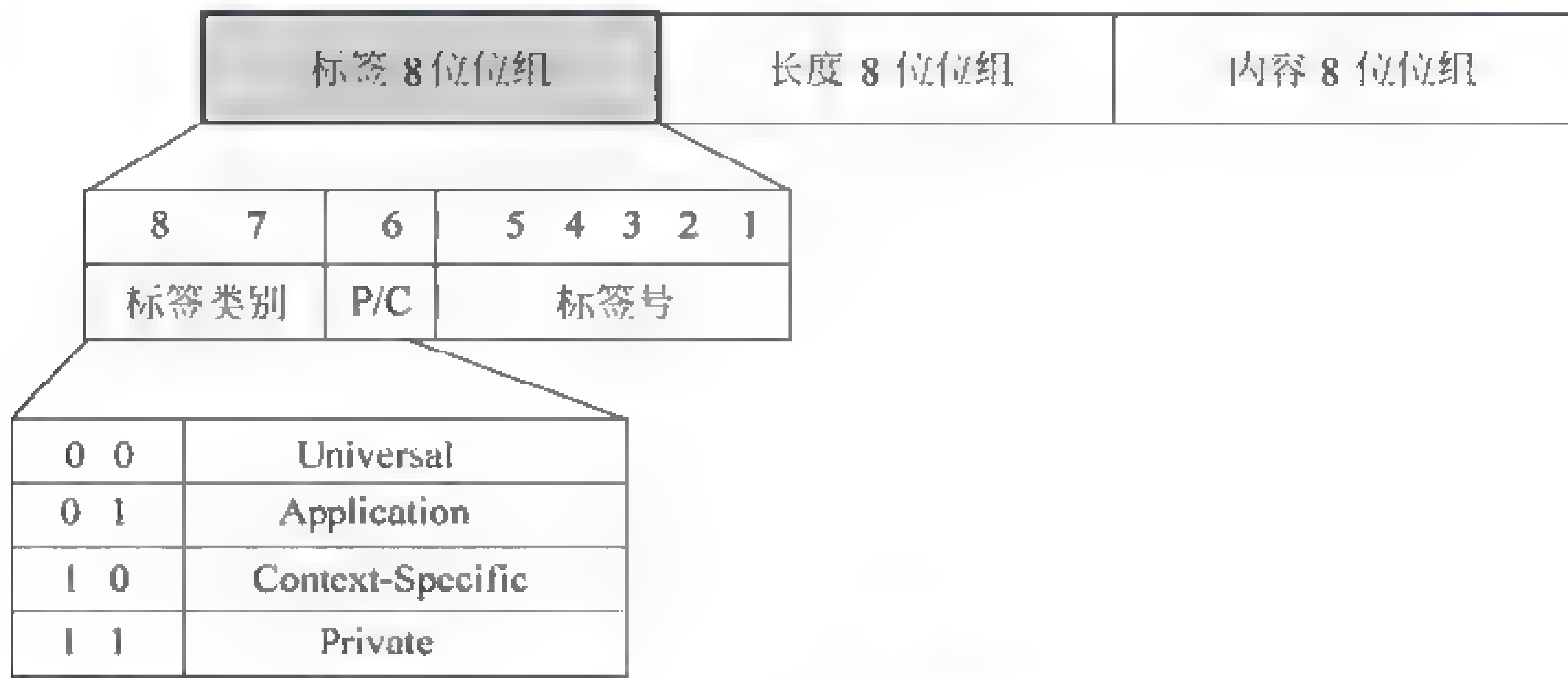


图1-119　TLV编码格式

1．标签字段

标签字段对标签类别、标签号和编码格式进行编码。其格式如图1-119所示。标签类别用二位表示，共有4类标签。这4类标签的编码如图1-119所示。

另外用1位P/C指明编码格式：0代表简单类型，1代表构造类型。简单编码是一个数据值编码，其值可用8位位组直接表示这个数据值。而构造编码的值可用多个8位位组数据值进行编码。不同类型的数据值可能是简单的，也可能是构造的。如果标签号在0～30之间，则标签号可以用其余5位比特表示。当标签号大于30时，标签字段就需要一个以上的字节。这时需要将标签字段的第一个8位位组的后5位全部置1，标签字段的后继8位位组除最后一个外，最高位均置1。这样将后继8位位组的低7位连接在一起就可以得到标签号。并且第一个后继8位位组不能所有位全为0，这是为了保证标签号的编码长度最短。

2．长度字段

长度字段用来表示值字段的8位位组数。根据值字段的长度在编码时是否可知，长度字段的编码可以分为确定格式（definite form）和不确定格式（indefinite form）。

对于确定格式，长度字段由一个或多个8位位组组成。当长度字段只包括一个8位位组时，可以表示小于128个8位位组的值字段的长度，这时称为短格式。短格式的长度字段8位位组的第8位为0，第7位至第1位是长度的编码（可以为0），编码值是无符号二进制整数，以第7位为最高有效位。例如，L=38的编码是（00100110）$_2$。

当值字段的精确长度已知，并且长度大于或等于 128 字节时，采用长格式。长格式将长度字段的第一个字节最高位置 1，其余 7 位表示后面有多少字节用来表示值字段的长度。其中后 7 位全 1 的值保留不使用，这是为了将来可能的扩展。在这种情况下，长度字段可能的最大长度是 127B，其中 126B 用来表示值字段的长度，这显然足够了。和短格式一样，长格式的编码值也是无符号二进制整数，以第 1 个后继 8 位位组的第 8 位为最高有效位。例如，L＝201 的编码是（1000000111001001）$_2$。

当内容字段的长度在编码时无法确定，则采用不确定格式。不确定格式使用以内容结束 8 位位组来标记编码的结束。不确定格式的长度字段是一个 8 位位组，第 8 位置 1，第 7 位至 1 位为 0，即（10000000）$_2$。当 8 位位组内容结束时，用两个连续的 8 位位组标识。

3．值字段

内容字段由 0 个或多个 8 位位组组成，并按不同类型数据值的不同规定对它们进行编码。

布尔值的编码应是简单类型的。值 8 位位组由 1 个 8 位位组组成。若布尔值是 FALSE，则 8 位位组是 00。若布尔值是 TRUE，8 位位组是 FF，由发送者选择。例如，布尔值 TRUE 的编码是 01 01 FF；布尔值 FALSE 的编码是 01 01 00。其中第一个字节表示布尔类型的标签（UNIVERSAL 1）号，第二个字节指明值部分的长度为 1 个字节。

整数值的编码应是简单类型的。值 8 位位组由一个或多个 8 位位组组成。整数值采用二进制补码形式编码。补码从高位到低位排列在值的第一字节的第 8 位到第 1 位，第二字节的第 8 位到第 1 位，以下按顺序类推。编码取需要的最少字节数，因此不可能出现第一字节的所有位和第二字节的第 8 位全 0 或全 1 的情况。ASN.1 的其他数据类型的编码方式请参考相关书籍。

1.9.2.3　管理信息结构（SMI）

经 SNMP 协议传输的所有管理信息都被收集到一个或多个管理信息库（MIB）中，被管对象类型按照 SMI 和标识定义。管理信息结构主要包括以下三个方面。

- 对象的标识，即对象的名字。SMI 采用的是层次型的对象命名规则，所有对象构成一棵命名树，连接树根节点至对象所在节点路径上所有节点标识便构成了该对象的对象标识符。
- 对象的语法，即如何描述对象的信息。对象的信息表示采用的是抽象语法表示的子集，同时也针对 SNMP 的需要作了一定的扩充。表示管理对象至少需要包括 4 个方面的属性：类型、存取方式、状态和对象标识。
- 对象的编码。代理和管理站之间进行通信必须对对象信息统一编码，为此，SMI 规定了对象信息的编码采用基本编码规则。

被管对象被定义为所代表的资源的管理视图。一个资源的管理视图不是对资源的简单观察结果，而要对它进行取舍和加工，即要对其进行管理说明，确定资源的哪些方面

由管理者监控。因此，被管对象不是被管资源的代名词，而是定义了一个资源的一般操作之外的管理能力。

1．对象的标识

SMI 明确要求所有被管理的信息和数据都要由管理树来标识，如图 1-120 所示。这棵管理树来源于 OSI 的定义，它具有从根开始的严格分层化结构。管理树的分支和叶子是用数字和名字两种方式显示的。在管理树中通向一个节点或叶子的路径是用对象标识符表示的。树中的各个分支是用数值表示的，因此对象标识符就构成了一个整数序列，中间是以“.”号间隔而成的。

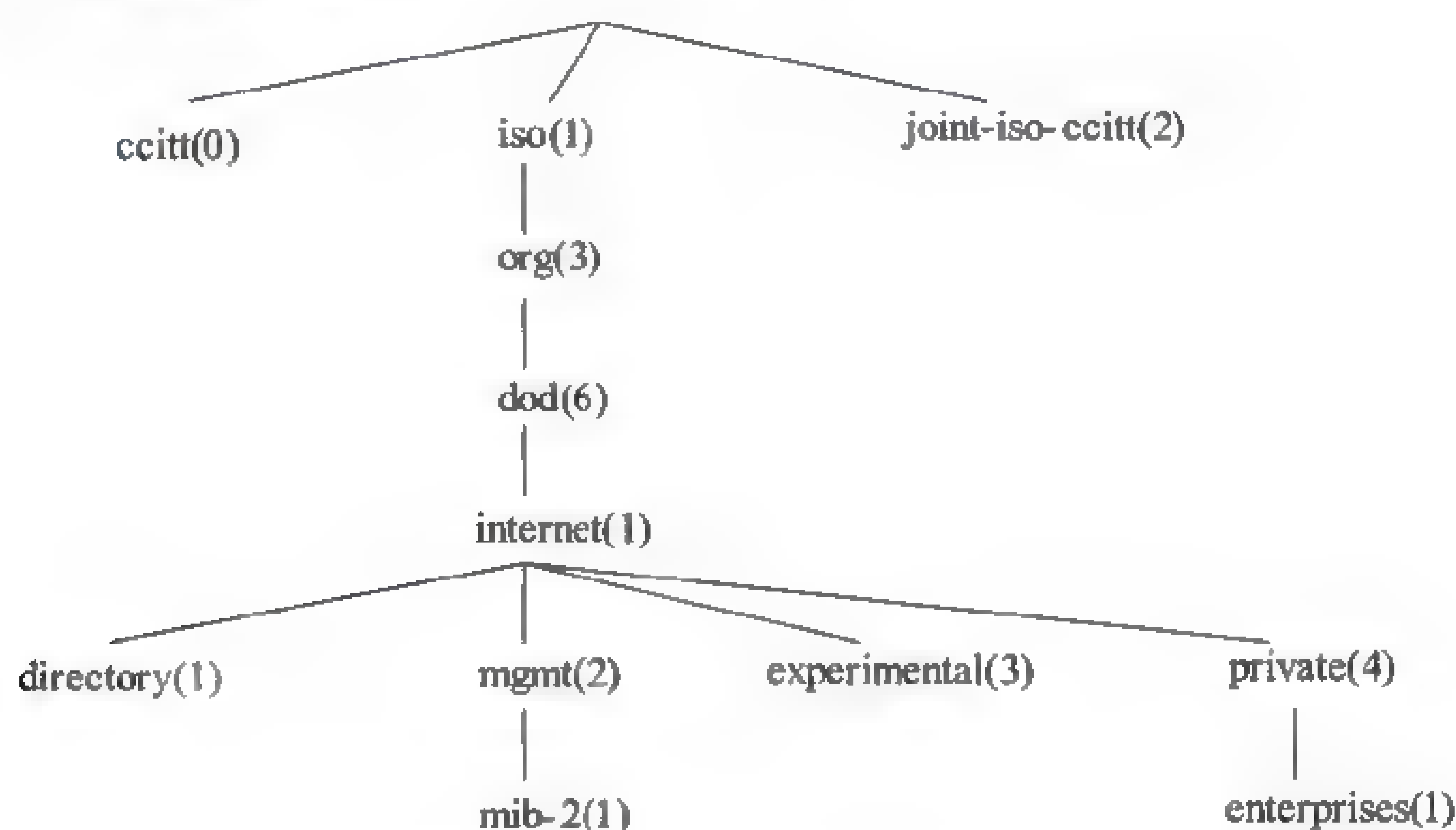


图 1-120　MIB 树型结构

管理树的根节点是一个虚拟节点，没有实际对应的名字和编码。处于叶子位置上的对象是实际的被管对象，每个实际的被管对象表示某些被管资源、活动或相关信息。树型结构本身定义了一个将对象组织到逻辑上相关的集合之中的方法。

在 MIB 中每个对象都被赋予一个对象标识符（object identifier），以此命名对象。由于对象标识符的值是层次结构的，因此命名方法本身也能用于确认对象的结构。如图 1-120 所示，从根节点开始，第一级有三个节点：国际电报电话咨询委员会 ccitt 分支、国际标准化组织 iso 分支和 joint-iso-ccitt 分支。通常使用的管理信息都是在 iso（1）子树下面定义，其中包括 ISO 为其他组织定义的子树 org（3）。在 org（3）节点下的一个子树是美国国防部使用的 dod（6），而在该节点下的子节点 internet（1）定义了所有 Internet 所使用的协议，包含了与因特网有关的所有的管理对象，该子树由 IAB 统一管理，其完整的对象标识符为 1.3.6.1。在 internet 节点下定义了 4 个子树：directory（1）、mgmt（2）、experimental（3）和 private（4）。

SNMP 定义的管理对象全部在节点 internet 下，internet 的对象标识符是：

internet　OBJECT　IDENTIFIER::={iso（1）　org（3）　dod（6）1}　　--或者 1.3.6.1

因此 SNMP 管理对象的对象标识符都是以前缀 1.3.6.1 开始，所以在定义 MIB 的 RFC 中都略去了这一前缀，而以 internet 作为默认的公共前缀，对象标识符简记为父节点的名字标识和本节点的数字标识，如下所示。

mgmt　OBJECT IDENTIFIER::={internet 2}
mib-2　OBJECT IDENTIFIER::={mgmt 1}
system　OBJECT IDENTIFIER::={mib-2 1}
sysName OBJECT IDENTIFIER::={system 5}

2．管理信息结构的定义

1）模块定义

ASN.1 的基本单位是模块，用于定义一个抽象数据类型，ASN.1 模块实际上是由一组类型定义和值定义组成。类型定义就是说明类型的名称和类型的格式，值定义是规定将什么样的具体值赋给某一类型。模块定义的基本形式为：

```
<moduleIdentifier> DEFINITIONS ::=
               BEGIN
                   EXPORTS
                   IMPORTS
                   AssignmentList
               END
```

其中的 moduleIdentifier 是模块名，模块名的第一个字母必须大写。EXPORTS 结构用于定义其他模块可以移植的类型或值。而 IMPORTS 结构规定了模块中某些定义是从其他模块中移植过来的。 AssignmentList 部分包含模块定义的所有类型、值和宏定义。

2）宏表示

ASN.1 宏提供了创建“模板”用来定义宏的方法，MIB 对象就是采用宏定义模板来定义。这一小节介绍定义宏的方法，为此我们需要区分三个不同的概念。

- 宏表示：ASN.1 提供的一种表示机制，用于定义宏。
- 宏定义：用宏表示定义的一个宏，代表一个宏实例的集合。
- 宏实例：用具体的值代替宏定义中的变量而产生的实例，代表一种具体的类型。

宏定义的模板形式如下：

```
<macroname> MACRO::=
  BEGIN
      TYPE  NOTATION ::=<user defined type notation>
      VALUE  NOTATION ::-<user defined value notation>
      <supporting syntax>
  END
```

其中 macroname 是宏的名字，必须全部大写。宏定义由类型表示（TYPE NOTATION）、值表示（VALUE NOTATION）和支持产生式（supporting syntax ）三部分组成，而最后部分是任选的，是关于宏定义体中类型的详细语法说明。这三部分都由 Backus-Naur 范式说明。当用一个具体的值代替宏定义中的变量或参数时就产生了宏实例，它表示一个实际的 ASN.1 类型（叫做返回的类型），并且规定了该类型可取的值的集合（叫做返回的值）。可见宏定义可以看做是类型的类型，或者说是超类型。另一方面也可以把宏定义看做是类型的模板，用这种模板制造出形式相似、语义相关的许多数据类型。这就是宏定义的主要用处。

下面是取自 RFC1212 的关于对象类型的宏 OBJECT-TYPE 的定义，其中包含多个支持产生式。

```
OBJECT  -TYPE MACRO::=
  BEGIN
    TYPE NOTATION ::= "Syntax" type (TYPE ObjectSyntax)
                      "ACCESS" Access
                      "STATUS" Status
                       DescrPart
                        ReferPart
                        IndexPart
                        DefValPart
    VALUE NOTATION ::= value  (VALUE ObjectName)
    Access::="read-only" | "read-write" | "write-only" | "not-accessible"
    Status::= "mandatory" | "optional" | " obsolete"
    DescrPart ::=" DESCRIPTION" value (description DisplayString) | empty
    ReferPart ::= " REFERENCE" value (reference DisplayString) | empty
    IndexPart ::=   " INDEX" " {" IndexTypes " }" | empty
    IndexTypes ::=IndexType | IndexTypes "," IndexType
    IndexType ::=value (indexobject ObjectName) | type (indextype)
    DefValPart ::="DEFVAL" " {" value (defvalue ObjectSyntax) "}" | empty
    DisplayString::=OCTET STRING SIZE (0..255)
  END
```

TYPE NOTATION 包含 7 个子句，其中前 3 个是必选的，每个子句都描述对象的不同属性，具体解释如下。

- SYNTAX：表示对象类型的抽象语法，在宏实例中关键字 type 应由 ObjectSyntax 代替，即上面提到的通用类型和应用类型。我们有：

```
ObjectSyntax ::=CHOICE { simple     SimpleSyntax,
                      application-wide  ApplicationSyntax}
```

SimpleSyntax 是指 5 种通用类型，而 ApplicationSyntax 是指 6 种应用类型。

- ACCESS：定义 SNMP 协议访问对象的方式。可选择的访问方式有只读（read-only）、读写（read-write）、只写（write-only）和不可访问（not-accessible）4 种，这是通过访问子句定义的。任何实现必须支持宏定义实例中定义的访问方式，还可以增加其他访问方式，但不能减少。
- STATUS：说明实现是否支持这种对象。状态子句中定义了必要的（mandatory）和任选的（optional）两种支持程度。过时的（obsolete）是指老标准支持而新标准不支持的类型。如果一个对象被说明为可取消的（deprecated），则表示当前必须支持这种对象，但在将来的标准中可能被取消。
- DescrPart：这个子句是任选的，用文字说明对象类型的含义。
- ReferPart：这个子句也是任选的，用文字说明可参考在其他 MIB 模块中定义的对象。
- IndexPart：用于定义表对象的索引项。
- DefValPart：定义了对象实例默认值，这个子句是任选的。

最后一部分是值的产生式规则，该部分也是任选的。

3）宏实例的定义

当用一个具体的值代替宏定义中的变量（或参数）时就产生了宏实例，它表示一个实际的 ASN.1 类型（叫做返回的类型），并且规定了该类型可取的值的集合（叫做返回的值）。宏实例（即 ASN.1 类型）的定义首先是对象名，然后是宏定义的名字，最后是宏定义规定的宏体部分。下面给出对象定义的例子。

```
tcpMaxConn OBJECT-TYPE
        SYNTAX   INTEGER
        ACCESS    read-only
        STATUS    mandatory
        DESCRIPTION
        "The limit on the total number of TCP connection the entity can support"
        ::={tcp 4}
```

1.9.2.4 管理信息库（MIB）

1988 年 8 月，在 RFC1066 中公布了第一组被管对象，被认为是 MIB-1，它包括了 8 个对象组，约 100 个对象。

```
system       OBJECT IDENTIFIER ::= { mib 1 }
interfaces   OBJECT IDENTIFIER ::= { mib 2 }
at           OBJECT IDENTIFIER ::= { mib 3 }
```

ip   OBJECT IDENTIFIER ::= { mib 4 }
icmp   OBJECT IDENTIFIER ::= { mib 5 }
tcp   OBJECT IDENTIFIER ::= { mib 6 }
udp   OBJECT IDENTIFIER ::= { mib 7 }
egp   OBJECT IDENTIFIER ::= { mib 8 }

厂商很快就接受了 MIB-1，在他们实现的管理站和代理中把它作为开发成本合适的 SNMP 协议的基础。然而，不久以后，一个问题就变得非常突出，对一个网络管理系统而言，100 多个变量只能表示整个网络的一小部分。

1990 年 5 月，在 RFC1158 中公布了 MIB-2。MIB-2 引入了 cmot、transmission、snmp 这三个新的对象组，从而扩展了 MIB-1 已有的对象组。

MIB-2 除了引入新的对象组，还引入了很多新的对象，它们有：

- system 组中增加 sysContact、sysName、sysLocation 和 sysServices 这 4 个对象。
- interfaces 组的表对象 ifTable 中增加 ifSpecific 对象。
- ip 组的表对象 ipAddrTable 中增加 ipAdEntReasmMaxSize 对象，表对象 ipRoutingTable 中增加 ipRouteMask 对象，而且增加表对象 ipNetToMediaTable。
- tcp 组中增加 tcpInErrs 和 tcpOutRsts。
- udp 组中增加表对象 udpTable。
- egp 组中增加 egpAs 对象。

在 RFC1213 中，MIB-2 被彻底修订并采纳 RFC1212 中的简洁 MIB 定义，这一文档使 RFC1158 失效。RFC1213 在以下方面做了修订：

（1）修改文本，使 MIB 显示没有歧义，引入了 DisplayString 数据类型。

（2）与 SMI/MIB 和 SNMP 更强的向下兼容性。例如可取消的（depreciated）对象的引用，MIB 就可以知道某些对象已经在后来的版本标准中删除。MIB-2 中，将 at 组中的对象标记为可取消的对象。

（3）增强对多协议环境的支持。在多协议网络中的 MIB 必须能够支持多个地址映射表。

（4）创建适应各具体实现的 MIB 附加选项，例如在具体实现中可以用指定的正整数标识 IP 地址和路由表。

管理信息库的第一个版本 MIB-1 目前已经被在 RFC1213 中定义的 MIB-2 所取代，MIB-2 保留了 MIB-1 的对象标识符。图 1-121 显示了 MIB-2 的结构。

需要说明的是，MIB-2 包含了 11 个组，其中，地址转换组 at（3）已经废弃了多年，并且将随着 RFC1213 的引退而消失，CMOT 的开发也陷入停顿状态。对象组的具体描述如表 1-17 所示。

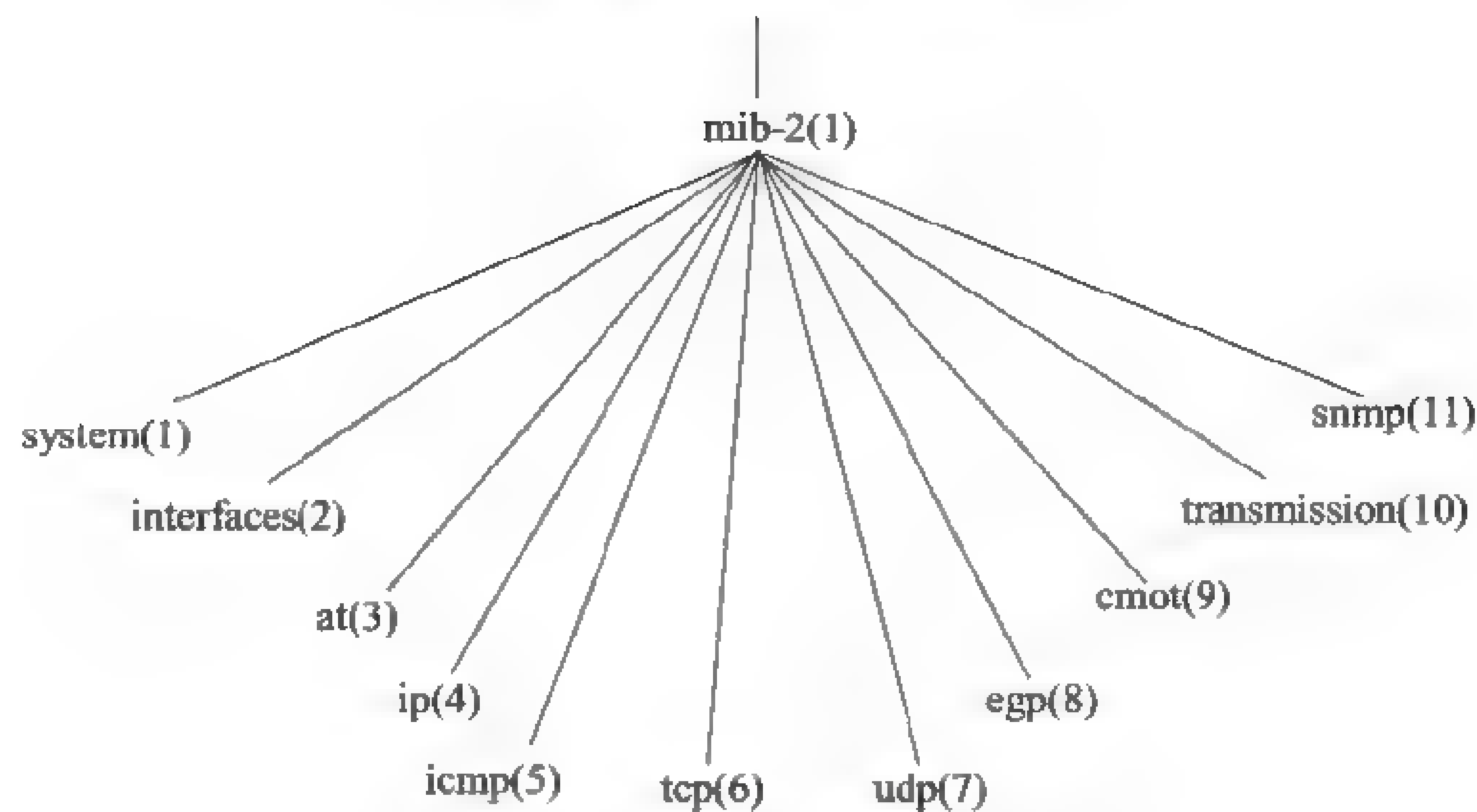


图 1-121　MIB-2 中的组及部分对象

表 1-17　MIB-2 对象组信息

对象组类别	描　述	管 理 功 能
system（1）	系统设备的整体信息	配置、故障
interfaces（2）	网络接口设备信息	配置、性能、故障、计费
ip（4）	系统中 IP 实现和运行信息	配置、性能、故障、计费
icmp（5）	系统中 ICMP 实现和运行信息	配置、性能、故障
tcp（6）	系统中 TCP 实现和运行信息	配置、性能、计费、安全
udp（7）	系统中 UDP 实现和运行信息	配置、性能、计费、安全
egp（8）	系统中 EGP 实现和运行信息	配置、性能、故障
transmission（10）	提供与子网类型有关的专用信息	配置、性能、故障、计费
snmp（11）	系统中 SNMP 实现和运行信息	配置、性能、故障、计费、安全

1.9.3　简单网络管理协议

1．SNMP 原理

简单网络管理协议（SNMP）是专门设计用来管理网络设备（服务器、工作站、路由器、交换机及 HUBS 等）的一种标准协议，它是一种应用层协议。SNMP 使网络管理员能够管理网络运行，发现并解决网络问题以及规划网络发展。通过 SNMP 接收循环消息(及事件报告)网络管理系统获知网络出现问题。目前 SNMP 有三种版本 SNMPv1、SNMPv2、SNMPv3。

图 1-122 给出了 Internet 网络管理的体系结构。由于 SNMP 定义为应用层协议，所以它依赖于 UDP 数据报服务。同时 SNMP 实体向管理应用程序提供服务，它的作用是把管理应用程序的服务调用变成对应的 SNMP 协议数据单元，并利用 UDP 数据报发送出去。

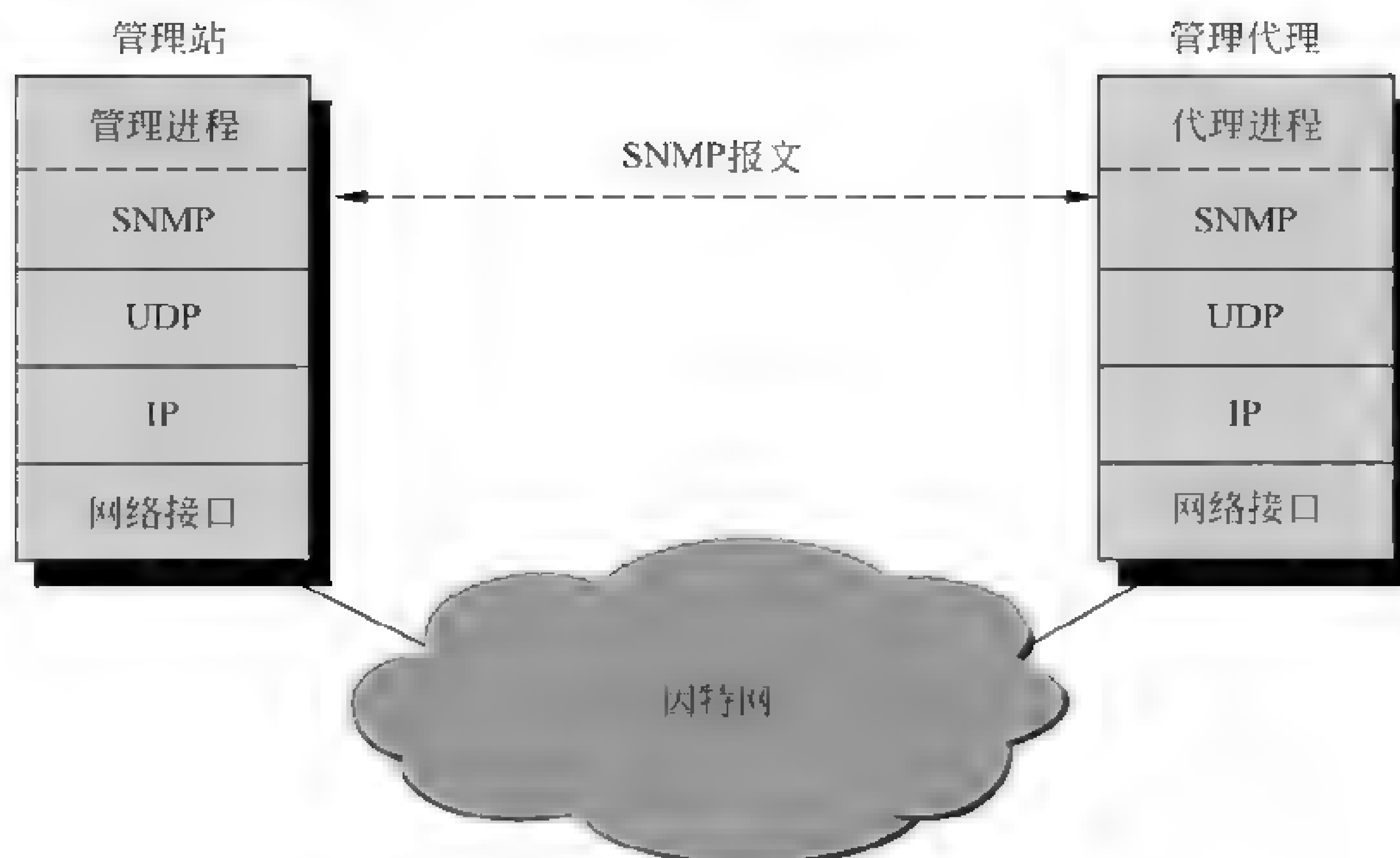


图 1-122　简单网络管理协议的体系结构

之所以选择 UDP 协议而不是 TCP 协议，这是因为 UDP 效率较高，这样实现网络管理不会太多地增加网络负载。但由于 UDP 不是很可靠，所以 SNMP 报文容易丢失。为此，对 SNMP 实现的建议是对每个管理信息要装配单独的数据报独立发送，而且报文应短些，不超过 484 个字节。

每个代理进程管理若干管理对象，并且与某些管理站建立团体（community）关系，如图 1-123 所示。团体名作为团体的全局标识符，是一种简单的身份认证手段。一般来说代理进程不接受没有通过团体名验证的报文，这样可以防止假冒的管理命令，同时在团体内部也可以实行专用的管理策略。

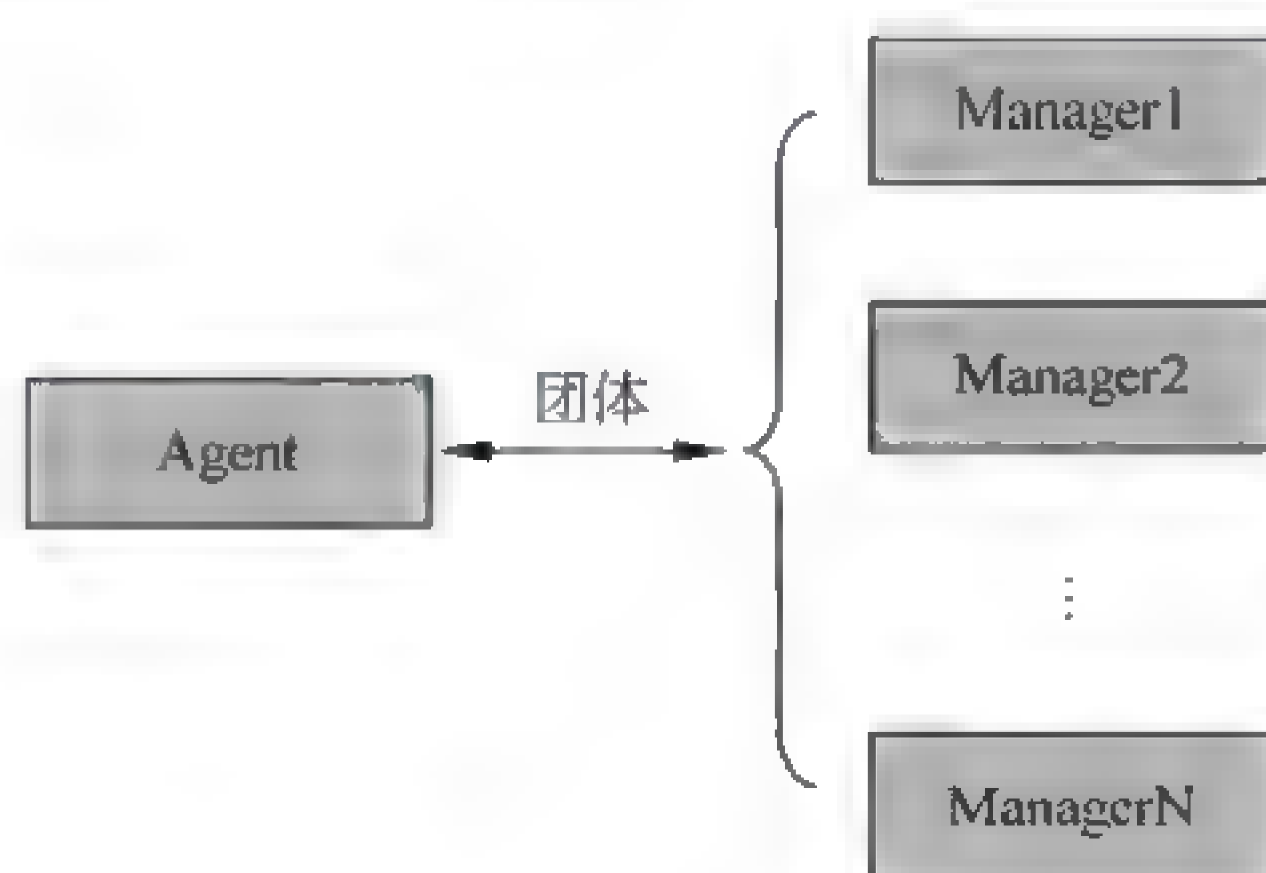


图 1-123　SNMPv1 的团体关系

SNMP 规定了 5 种协议数据单元 PDU（也就是 SNMP 报文），用来在管理进程和代理之间的交换。

（1）GetRequest 操作：从代理进程处提取一个或多个参数值。

（2）GetNextRequest 操作：从代理进程处提取紧跟当前参数值的下一个参数值。

（3）SetRequest 操作：设置代理进程的一个或多个参数值。

（4）GetResponse 操作：返回的一个或多个参数值。这个操作是由代理进程发出的，它是前面三种操作的响应操作。

（5）Trap 操作：代理进程主动发出的报文，通知管理进程有某些事情发生。

前面的三种操作是由管理进程向代理进程发出的，后面的两个操作是代理进程发给管理进程的，为了简化起见，前面三个操作今后叫做 Get、GetNext 和 Set 操作。

图 1-124 描述了 SNMP 的 5 种报文操作。请注意，在代理进程端是用熟知端口 161 来接收 Get 或 Set 报文，而在管理进程端是用熟知端口 162 来接收 Trap 报文。

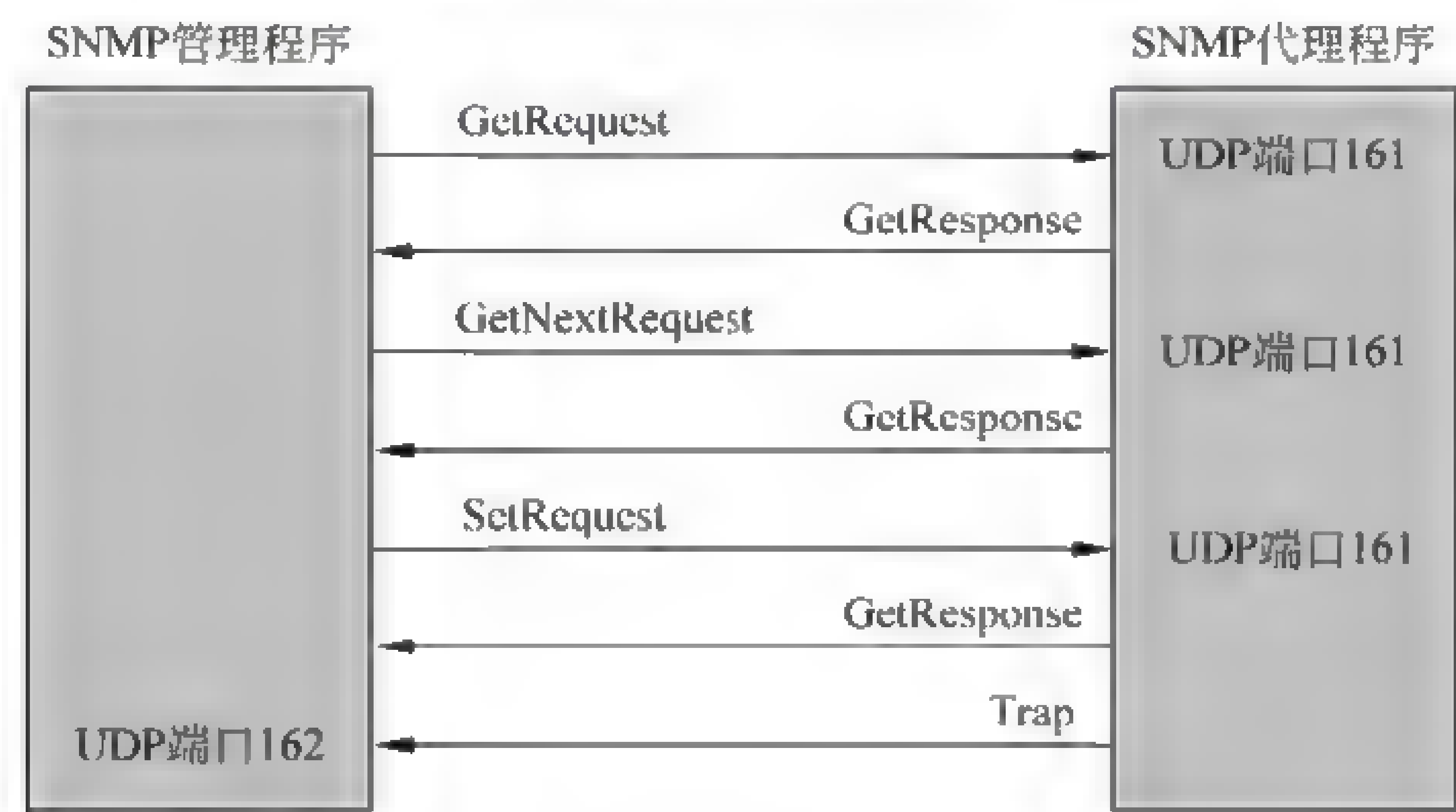


图 1-124　SNMP 的 5 种报文操作

SNMP 管理员使用 GetRequest 从拥有 SNMP 代理的网络设备中检索信息，SNMP 代理以 GetResponse 消息响应 GetRequest。可以交换的信息很多，如系统的名字，系统自启动后正常运行的时间，系统中的网络接口数等等。

GetRequest 和 GetNextRequest 结合起来使用可以获得一个表中的对象。GetRequest 取回一个特定对象；而使用 GetNextRequest 则是请求表中的下一个对象。

使用 SetRequest 可以对一个设备中的参数进行远程配置。SetRequest 可以设置设备的名字，关掉一个端口或清除一个地址解析表中的项。

Trap 即 SNMP 陷阱，是 SNMP 代理发送给管理站的非请求消息。这些消息告知管理站本设备发生了一个特定事件，如端口失败、掉电重启等，管理站可相应的作出处理。

2．SNMP 报文格式

SNMP 报文共有三个部分组成，即公共 SNMP 首部、Get/Set 首部、Trap 首部、变量绑定。SNMP 报文格式如图 1-125 所示。

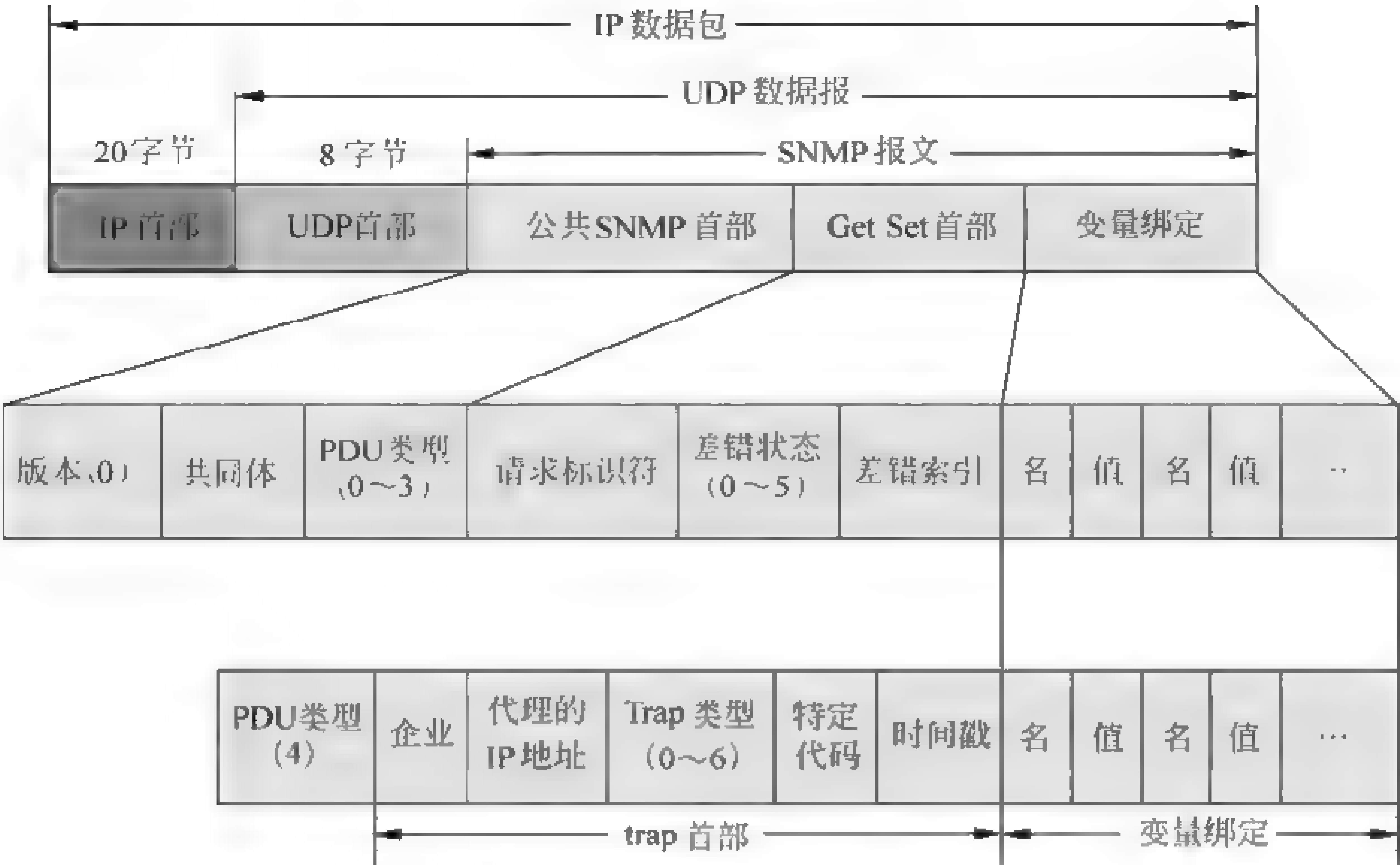


图 1-125 SNMP 报文格式

1）公共 SNMP 首部

公共 SNMP 共三个字段。

- 版本：写入版本字段的是版本号减 1，对于 SNMP（即 SNMPv1）则应写入 0。
- 团体：团体就是一个字符串，作为管理进程和代理进程之间的明文口令，常用的是 6 个字符 public。代理进程允许客户进程用制度团体名对变量进行操作，用读写团体名对变量进行读和写的操作。
- PDU 类型：根据 PDU 的类型，填入 0～4 中的一个数字，对应关系如表 1-18 所示。

表 1-18 PDU 类型

PDU 类型	名 称
0	GetRequest
1	GetNextRequest
2	GetResponse
3	SetRequest
4	Trap

2）Get/Set 首部

请求标识符（request ID）：这是由管理进程设置的一个整数值。代理进程在发送 GetResponse 报文时也要返回此请求标识符。管理进程可同时向许多代理发出 Get 报文，

这些报文都使用 UDP 传送，先发送的有可能后到达。请求标识符的作用在于其使得管理进程能够识别返回的响应报文对于哪一个请求报文。

差错状态（error status）：由代理进程回答时填入 0～5 中的一个数字。

差错索引（error index）：当出现 noSuchName、badValue 或 readOnly 的差错时，由代理进程在回答时设置的一个整数，它指明有差错的变量在变量列表中的偏移。

3）Trap 首部

企业（enterprise）：填入 Trap 报文的网络设备的对象标识符。

Trap 类型：此字段正式的名称是 generic-Trap，共分为表 1-19 中的 7 种。

表 1-19　Trap 类型字段

Trap 类型	名　字	说　明
0	ColdStart	代理进行了初始化
1	WarmStart	代理进行了重新初始化
2	LinkDown	一个接口从工作状态变为故障状态
3	Linkup	一个接口从故障状态变为工作状态
4	AuthenticationFailure	从 SNMP 管理进程接收到具有一个无效团体的报文
5	EgpNeighborLoss	一个 EGP 相邻路由器变为故障状态
6	EnterpriseSpecific	代理自定义的事件，需要用后面的“特定代码”来指明

特定代码（specific-code）：指明代理自定义的时间（若 Trap 类型为 6），否则为 0。

时间戳（timestamp）：指明自代理进程初始化到 Trap 报告的事件发生所经历的时间，单位为 10ms。例如时间戳为 1908 表明在代理初始化后 1908ms 发生了该时间。

4）变量绑定

在 SNMP 中，可以将多个同类操作（Get、Set、Trap）放在一个消息中。如果管理站希望得到一个代理处的一组标量对象的值，它可以发送一个消息请求所有的值，并通过获取一个应答得到所有的值。这样可以大大减少网络管理的通信负担。

为了实现多对象交换，所有的 SNMP 的 PDU 都包含了一个变量绑定字段。这个字段由对象实例的一个参考序列及这些对象的值构成。某些 PDU 只需给出对象实例的名字，如 Get 操作。对于这样的 PDU，接收协议实体将忽略变量绑定字段中的值。

3．SNMPv2

SNMPv2 的改进主要有以下三个方面：

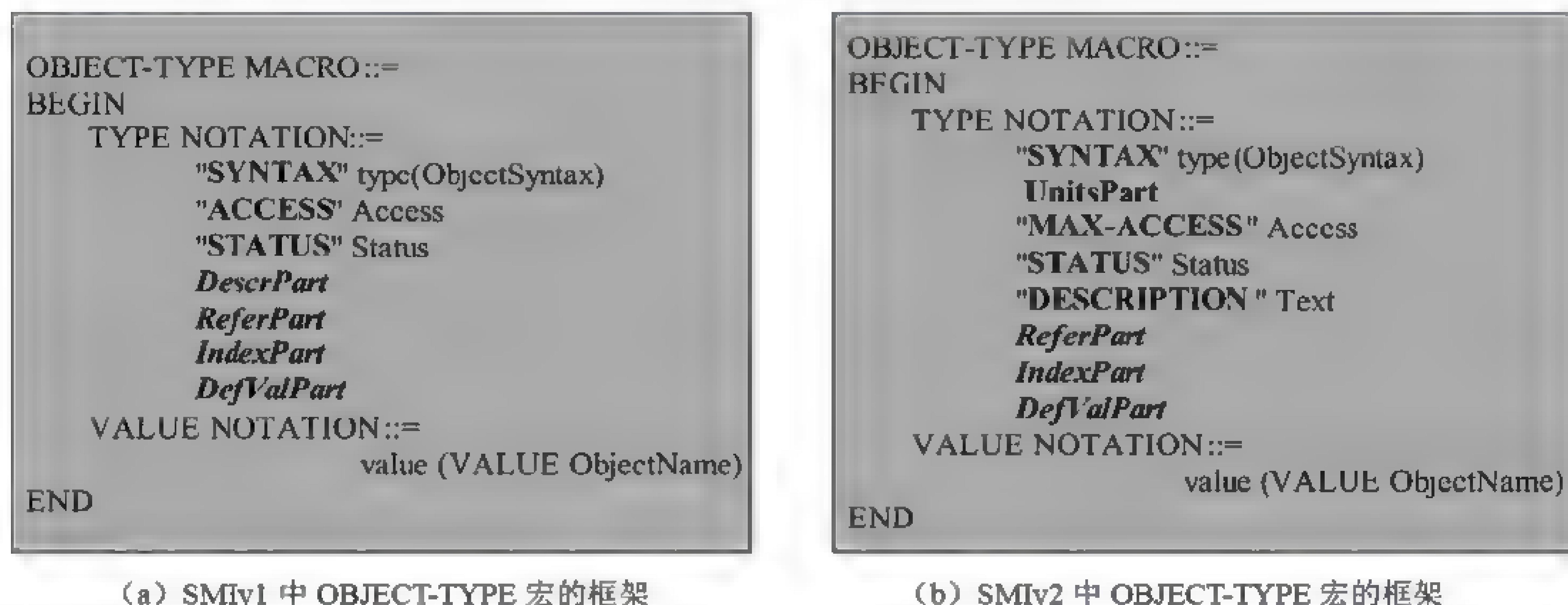
- 增加了 manager 和 manager 之间的信息交换机制，从而支持分布式管理结构。由中间（intermediate）manager 来分担主 manager 的任务，增加了远地站点的局部自主性。
- 改进了管理信息结构，例如提供了一次取回大量数据的能力，效率大大提高。
- 增强了管理信息通信协议的能力。可在多种网络协议上运行，如 OSI、Appletalk

和 IPX 等，适用多协议网络环境（默认网络协议是 UDP）。

SNMPv2 SMI 是对 SNMPv1 SMI 的改进，SMIv2 为被管理对象和 MIB 提供了更详尽的规范和文档。主要由对象定义、模块定义、通知定义和概念表组成。

1）对象定义

SNMPv2 的 OBJECT-TYPE 增加了新的内容。图 1-126（a）和图 1-126（b）分别给出了 OBJECT-TYPE 宏在 SMIv1 和 SMIv2 中的框架，其全文定义可以分别查阅 RFC1212 与 RFC2578。



```
OBJECT-TYPE MACRO::=
BEGIN
    TYPE NOTATION::=
           "SYNTAX" type(ObjectSyntax)
           "ACCESS" Access
           "STATUS" Status
           DescrPart
           ReferPart
           IndexPart
           DefValPart
    VALUE NOTATION::=
                      value (VALUE ObjectName)
END
```

（a）SMIv1 中 OBJECT-TYPE 宏的框架

```
OBJECT-TYPE MACRO::=
BEGIN
    TYPE NOTATION::=
           "SYNTAX" type(ObjectSyntax)
           UnitsPart
           "MAX-ACCESS" Access
           "STATUS" Status
           "DESCRIPTION " Text
           ReferPart
           IndexPart
           DefValPart
    VALUE NOTATION::=
                      value (VALUE ObjectName)
END
```

（b）SMIv2 中 OBJECT-TYPE 宏的框架

图 1-126　OBJECT-TYPE 宏在 SMIv1 和 SMIv2 中的框架

2）模块定义

SMIv2 包含三种信息模块。

- MIB 模块：包含一组有关的管理对象的定义。MIB 模块用到了 OBJECT-IDENTITY 宏和 MODULE-IDENTITY 宏。
- MIB 一致性声明模块：使用 OBJECT-GROUP、NOTIFICATION-GROUP 和 MODULE-COMPLIANCE 宏说明有关管理对象实现方面的最小要求。
- 代理能力说明模块：用 AGENT-CAPABILITIES 宏说明代理实体应该实现的能力。

3）通知定义

SNMPv2 提供了通知类型的宏定义 NOTIFICATION-TYPE，用于定义异常条件出现时 SNMPv2 实体发送的信息。任选的 OBJECT 子句定义了包含通知实例中 MIB 对象序列。下面就分别给出 NOTIFICATION-TYPE 宏定义的框架。

```
NOTIFICATION-TYPE MACRO ::=
BEGIN
   TYPE NOTATION ::=
             ObjectsPart
```

```
                "STATUS" Status
                "DESCRIPTION" Text
                ReferPart
    VALUE NOTATION ::=
                value (VALUE NotificationName)
    ObjectsPart ::=
                "OBJECTS" "{" Objects "}"| empty
    Objects ::=
                Object| Objects "," Object
    Object ::=
                value (ObjectName)
    Status ::=
                "current"| "deprecated"| "obsolete"
    ReferPart ::=
                "REFERENCE" Text| empty
    Text ::= value (IA5String)
END
```

其中，ObjectsPart 是可选项子句，定义每个通告实例所包含的 MIB 对象排序后的顺序，这些对象的取值存放在 PDU 的 variable-bindings 中传送到管理站。一般用于向管理站提供具体的警报相关数据和信息。ReferPart 也是可选项子句，用来描述参考信息。

4）概念表

SNMPv2 的管理操作只能作用于标量对象，复杂的信息要用表来表示。按照 SNMPv2 规范，表是行的序列，而行是列对象的序列。SNMPv2 把表分为以下两类。

- 禁止删除和生成行的表：这种表的最高访问级别是 read-write。在很多情况下这种表由代理控制，表中只包含 read-only 型的对象。
- 允许删除和生成行的表：这种表开始时可能没有行，有管理站生成和删除行。行数可由管理站或代理改变。

在 SNMPv2 表的定义中必须含有 INDEX 或 AUGMENTS 子句，但是只能有一个。AUGMENTS 子句的作用是表示概念行的扩展。AUGMENTS 子句的引入实质是在已定义的表对象的基础上通过增加列对象来定义新表，这样就不需要重新建立已有的行定义。

5）SNMPv2 报文格式

在 SNMPv2 消息中可以传送 7 类 PDU。图 1-127 描述了 SNMPv2 PDU 的格式。

值得注意的是，GetRequest、GetNextRequest、SetRequest、SNMPv2-Trap、Inform-Request 5 种 PDU 具有完全相同的格式，并且也可以看作是 error-status 和 error-index 两个字段被置 0 的 Response PDU 的格式。这样设计的目的是为了减少 SNMPv2 实体需要处理的 PDU 格式种类。

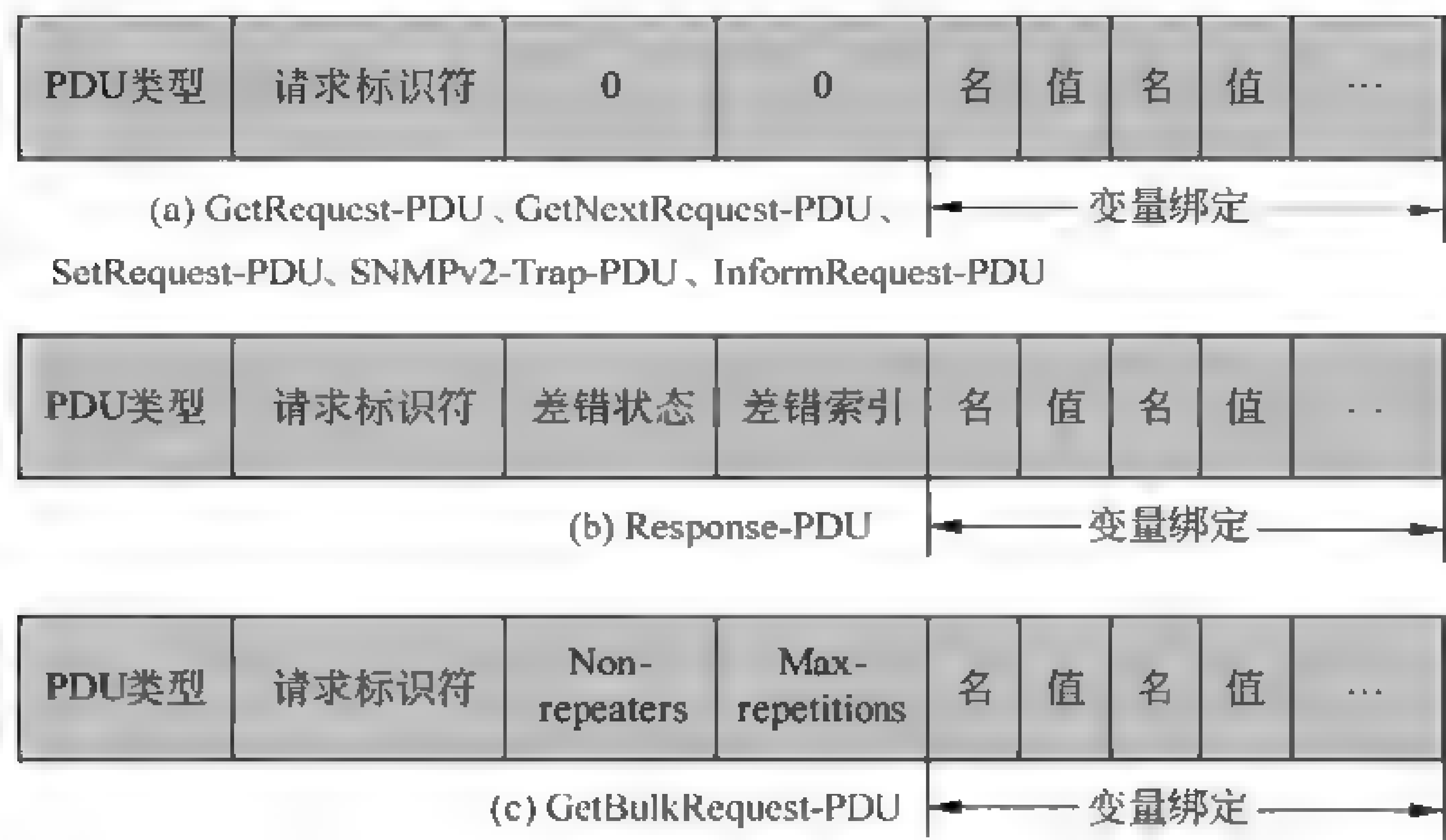


图 1-127　SNMPv2 PDU 格式

4．SNMPv3

1999 年 4 月发布的 SNMPv3 新标准，包含了全面的安全性技术。SNMPv3 定义了一种框架，用来把安全性整合到 SNMPv1 或 SNMPv2 的整体功能中。SNMPv3 只是一个安全规范，没有定义其他新的 SNMP 功能，只为 SNMPv1 和 SNMPv2 提供安全方面的功能。

RFC2271 定义的 SNMPv3 体系结构，体现了模块化的设计思想，可以简单地实现功能的增加和修改。其特点如下。

- 适应性强：适用于多种操作环境，既可以管理最简单的网络，实现基本的管理功能，又能够提供强大的网络管理功能，满足复杂网络的管理需求。
- 扩充性好：可以根据需要增加模块。
- 安全性好：具有多种安全处理模块。

在实现方面，对 SNMP 的体系结构会有以下不同的要求：

- 具有命令应答者和/或通报生成者应用的实体（最小的 SNMP）。
- 具有代管转发者应用的 SNMP 实体。
- 具有命令产生者和/或通报接收者应用的命令行驱动的 SNMP 实体。
- 具有命令生成者和/或通报接收者应用，并具有命令应答和/或通报产生者应用的 SNMP 实体（以往称为 SNMP 中间层管理者或双重角色实体）。
- 具有命令生成者和/或通报接收者，及为管理潜在的非常大量的被管节点可能的其他应用的 SNMP 实体（以往称为网络管理站）。

为了能够统一满足以上要求，SNMPv3 定义了一个可进化的体系结构框架。具体细节请参考相关书籍。

5．RMON

远程网络监视（Remote network MONitoring，RMON）是对 SNMP 标准的重要补充，是简单网络管理向互联网管理过渡的重要步骤。RMON 扩充了 SNMP 的管理信息库 MIB-2，可以提供有关互联网管理的重要信息，在不改变 SNMP 协议的条件下增强了网络管理的功能。从某种意义上说，RMON 的定义为网络的分布式管理提供了实现的可能性。

IETF 于 1991 年 11 月公布的 RFC1271 定义了 RMON MIB，对 SNMP 轮询的弊端进行了弥补，扩充了管理信息库 MIB-2，在不改变 SNMP 协议的条件下增强了网络管理的功能，进一步解决了 SNMP 在日益扩大的分布式网络中所面临的局限性。

RMON 规范主要是给出 RMON 管理信息库的定义。RMON MIB 由一组统计数据、分析数据和诊断数据构成，RMON MIB 的功能是对通过收集“RMON MIB 功能组”的信息进行管理。最早的 RMON 管理信息库，即 RMON1，主要包括以太网的各种统计数据，共有 9 个功能组，后来又扩展到其他网络类型，在 RFC1513-1993 中加入了令牌环网统计信息。虽然 RMON1 为远程监视提供了一个行之有效的手段，但它只能存储 MAC（media access control）层管理信息。从 1994 年开始对 RMON MIB 进行了扩充，使得能够监视 MAC 层之上 3～7 层的通信，这就是后来的 RMON2。目前的 RMON 管理信息结构包含 20 个功能组，如图 1-128 所示。

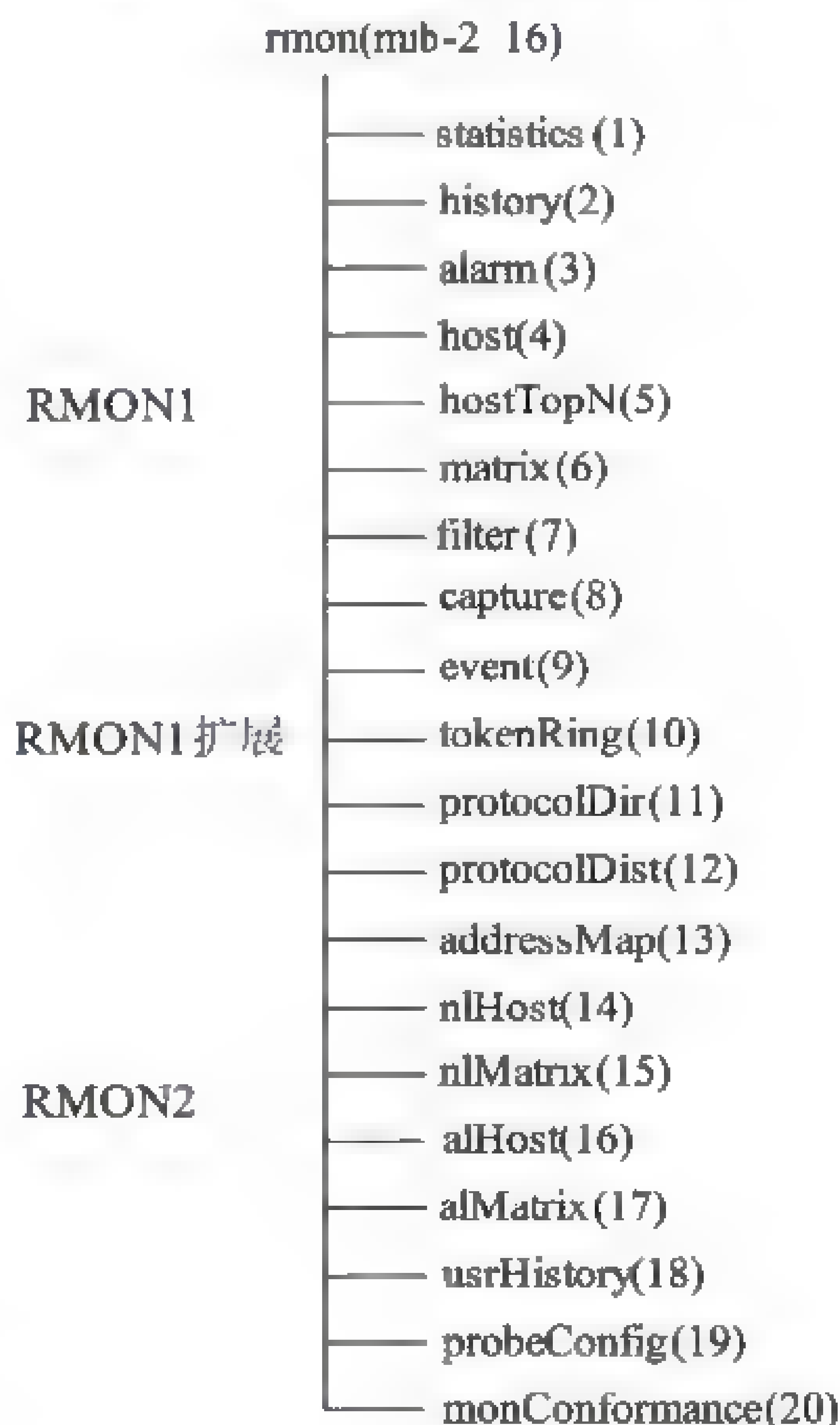


图 1-128　RMON MIB

6．SNMP 应用

在网络管理系统中，需要了解网络资源的状况，对它进行监视和控制。考虑到应用的实时性以及系统的开销，需要直接通过底层网络协议来实现。而 SNMP 正是采用面向无连接的用户数据报 UDP/IP 来实现其功能，实体间的通信无须先建立连接，降低了系统开销，并且现在的网络设备一般都支持 SNMP，具有 SNMP 的代理，这使得 SNMP 的实现成为可能。SNMP 在网络管理系统中主要应用如下：

（1）访问 MIB 库的变量并给出相应变量的描述。

（2）通过访问 SNMP MIB 可以获得网络性能的有关数据，对网络的性能和吞吐量分析。

（3）监测中心对监测设备进行查询来获得有关网络状态的信息，对网络性能进行动态分析，并进行设备监控，用于以后的评估和分析。

（4）在 SNMP 服务器上进行警告配置，网络中任何支持 SNMP-Trap 协议的 SNMP 设备都能收到警告。SNMP 是通过客户/服务器的方式来实现的。网络管理员在本地计算机上调用 SNMP 客户机，利用客户机与 1 个或多个运行在远程计算机上的 SNMP 服务器取得联系，从而实现故障管理功能。

下面将给出一个 SNMP 在网络管理中的应用例子，例子中用到了 Netsnmp 软件。Netsnmp 是目前网络主机上使用比较多的 SNMP 软件之一，可以在许多镜像网点下载。它作为网络管理应用软件，可通过 SNMP 协议中的命令，调用设备 MIB 库的对象标识符 OID 串，编写脚本集中提取设备的参数值，如 CPU 利用率、内存利用率、进程状态、时延、端口流量、性能参数等。

安装完成 Netsnmp 后，启动主机的 snmpd 进程，它成为一个带有管理器的 SNMP 实体了。

例：实时监测网络时延。

以 Cisco 设备为例，如图 1-129 所示，通过 192.168.1.4 这台主机对 Cisco 路由器 192.168.1.1 进行监控，实时监测其网络时延。

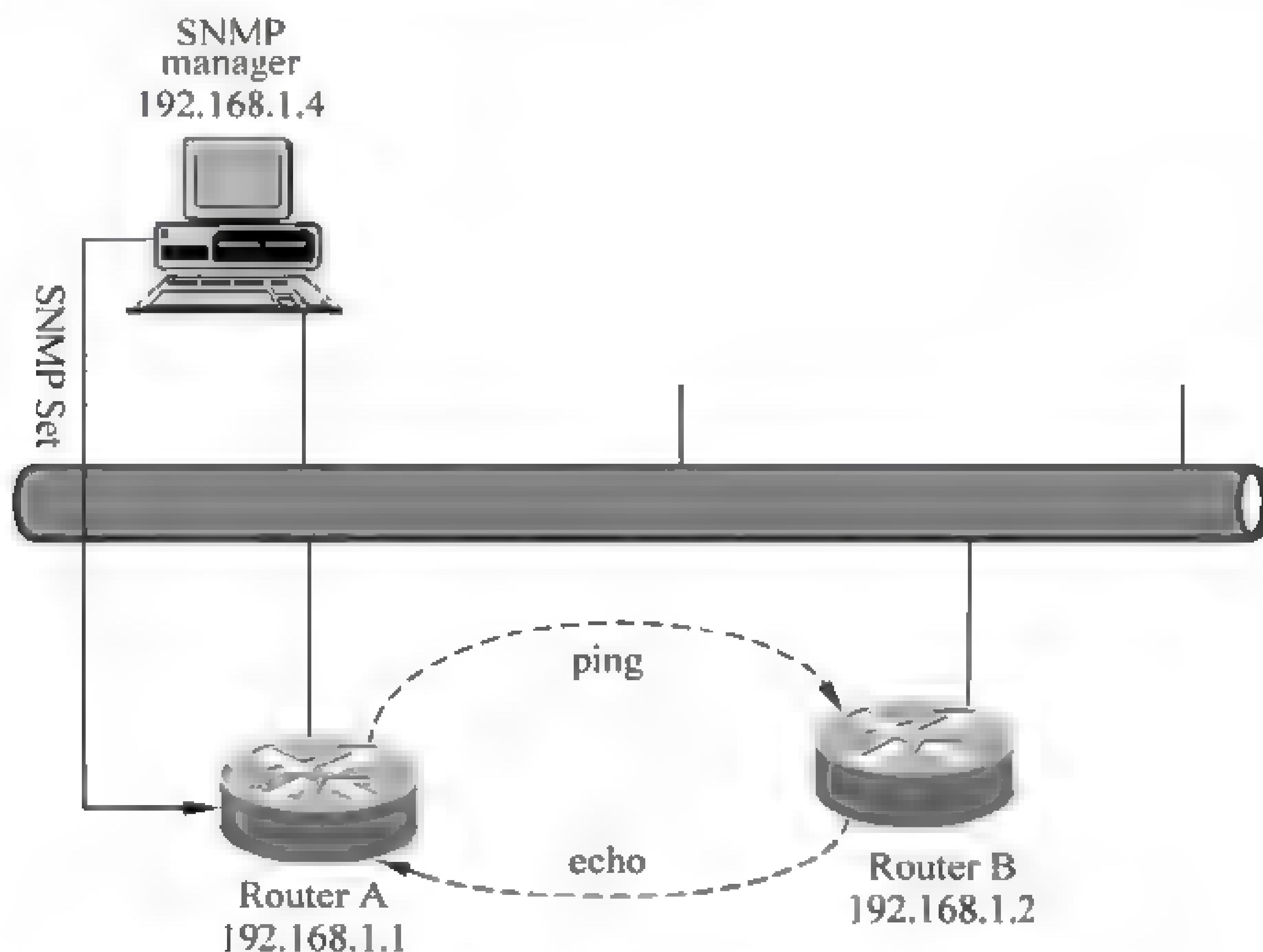


图 1-129 网络结构

在 Cisco 路由器上，配置 snmp server 和允许访问列表，使其接受 snmp manager 的管理。

```
!
snmp-server engineID local 00000009020000089A9E47FF
snmp-server community<8bits 字符串命名>RW81
snmp-server community<8bits 字符串命名>RO81
```

```
snmp-server enable traps
snmp-server host 192.168.1.4<上述被命名的 8bits 字符串之一>snmp
snmp-server trap-source loopback 0
access-list 81 permit 192.168.1.4
!
```

在管理站（192.168.1.4）上通过 snmp 协议对被管的路由器（192.168.1.1）的变量进行设置，得到路由器 A（192.168.1.1）到路由器 B（192.168.1.2）remote ping 的时延。管理站通过 snmp 命令的改变（snmpset），设置路由器 A 到路由器 B 的扩展 ping 变量，包括包数、包大小、超时时间等等；通过 SNMP 的检查（snmpwalk），得到返回的时延结果。

```
snmpset -v 1 -c private 192.168.1.1  1.3.6.1.4.1.9.9.16.1.1.1.16.
331 integer 6(破坏上次设置)
snmpset -v 1 -c private 192.168.1.1  1.3.6.1.4.1.9.9.16.1.1.1.16.
331 integer 5(重新创建)
snmpset -v 1 -c private 192.168.1.1  1.3.6.1.4.1.9.9.16.1.1.1.15.
331 s  "GSR12012"(设置 CiscoPingEntryOwner)
snmpset -v 1 -c private 192.168.1.1  1.3.6.1.4.1.9.9.16.1.1.1.2.
331 integer 1(设置协议为 IP)
snmpset -v 1 -c private 192.168.1.1  1.3.6.1.4.1.9.9.16.1.1.1.3.
331 x  "C0 A8 1 2"(设置目的地 192.168.1.2)
snmpset -v 1 -c private 192.168.1.1  1.3.6.1.4.1.9.9.16.1.1.1.6.
331 integer 1000(设置超时)
snmpset -v 1 -c private 192.168.1.1  1.3.6.1.4.1.9.9.16.1.1.1.4.
331 integer 10  (设置包数)
snmpset -v 1 -c private 192.168.1.1  1.3.6.1.4.1.9.9.16.1.1.1.5.
331 integer 111 (设置包大小)
snmpset -v 1 -c private 192.168.1.1  1.3.6.1.4.1.9.9.16.1.1.1.16.
331 integer 1 (激活开始执行命令动作)
snmpwalk -v 1 -c private 192.168.1.1  1.3.6.1.4.1.9.9.16.1.1.1.12.
331(得到返回时延为 1ms)
SNMPv2-SMI::enterprises.9.9.16.1.1.1.12.331  = INTEGER:1
```

编写脚本，就可以实现 192.168.1.4 这台主机对 Cisco 路由器 192.168.1.1 的远程监控。

1.9.4　网络管理工具

1.9.4.1　基于 Web 的管理

传统的网络管理界面是通过网络管理命令驱动的远程登录屏幕，必须由专业网络管理工作人员操作，使用和维护网络管理系统也需要专门培训的技术人员，网络功能复杂

化，使传统网络管理界面的友好程度愈来愈差。为了减轻网络管理复杂性，降低网络管理费用，急需研究和开发一种跨平台、方便、适用的新的网络管理模式，基于 Web 的网络管理模式可以实现这个目标。这种新的网络管理模式融合了 Web 技术、Java 技术和网络管理技术，它允许网络管理人员通过与万维网同样的形式去监测、管理他们的网络系统，并使用 Web 浏览器在网络任何节点上方便迅速地配置、控制及访问网络和它的各个部分，这种新的网络管理模式的魅力在于它是交叉平台，可以很好解决很多由于多平台结构产生的互操作问题，提供比传统网络管理更直接、更易于使用的图形界面，从而降低了对网络管理操作和维护人员的特别要求。

1. WBM 与传统网络管理平台的比较

随着 Intranet 的流行和发展，其本身的结构也变得越来越复杂，这大大增加了网络管理的工作量，也给网络管理员真正管理好 Intranet 带来了很大的困难。传统的网络管理方式已经不适应当前网络发展的趋势。作为一种全新的网络管理模式，基于 Web 的网络管理模式（Web-Based Management，WBM）可以允许网络管理人员使用任何一种 Web 浏览器，在网络任何节点上方便迅速地配置、控制以及存取网络和它的各个部分。WBM 从出现伊始就表现出强大的生命力，它以其特有的灵活性、易操作性等特点赢得了许多技术专家和用户的青睐。

（1）传统的管理者-代理集中管理模式存在以下缺陷。

- 由一个网管站（NMS）来负责收集分析所有被管资源的状态信息并进行相应管理，造成网管站工作负担过重，这没有充分发挥网络的分布计算资源优势。
- 所有的网络管理数据都必须传送给网管站分析处理，这样易在管理者端形成通信瓶颈。
- 当网络出现连接故障时，造成全网或局部失控。
- 由于系统规模和应用越来越复杂，加上用户需求的改变，现行的网络管理平台不易扩展升级。
- 由于网络采用不同厂商的网络设备、协议、操作系统及数据库，网管人员不得不分别借助各种孤立的管理工具来监视和控制网络的运行以及管理各种信息服务。这给网管人员带来了额外负担，给有效地管理好网络带来很大的困难。
- 目前网络管理的重心仍然放在管理网络的硬件设备上，缺乏真正有效的包括各种应用服务的集成网络管理。以前网络设备由于其处理能力和资源的缺乏，只能在其上运行一个简单的 SNMP 代理，而现在的网络设备含有更强的处理器和更多的内存，因此具有管理自身的能力。目前对 SNMP 有了一些改进措施，如采用 MIB 元变量、RMON、Agent X 等方法。

（2）基于 Web 的网络管理具有以下优点。

- 地理上和系统上的可移动性。基于 Web 网络管理的可移动性使管理员使用任何一个 Web 浏览器从 Intranet 的任意一台网络工作站都可以监测和控制内部网络。对

于网络管理系统的提供者来说，在一个平台上实现的管理系统可以从任何一台安装有 Web 浏览器的计算机上访问，不管这台计算机是服务器还是专用工作站，或是普通 PC，操作系统的类型也不受限制。

- 具有统一的网络管理程序界面。网络管理员不必像以往那样学习和运用不同厂商的网络管理系统程序的操作界面，而是通过简单且非常熟悉的 Web 浏览器进行操作，完成网络管理的各项任务。
- 网络管理平台具有独立性。WBM 的应用程序可以在各种环境下使用，包括不同的操作系统，体系结构和网络协议，无须进行系统移植。
- 网络管理系统之间可无缝连接。网络管理员可以通过浏览器在不同的管理系统之间进行切换，比如在厂商甲开发的网络性能管理系统和厂商乙开发的网络故障管理系统之间进行切换，使得两个系统能够平滑地相互结合，组成一个整体。

在网络管理领域，包括 IBM/Tivoli、Sun、HP 和 Cisco 等公司在内的网络管理系统软件供应商都竞相推出融合了 Web 技术的管理平台。

2．WBM 的实现方式

网络管理 Web 化的基本实现方案有两种。一种是基于代理的解决方案，另一种是嵌入式解决方案。

1）基于代理的解决方案

基于代理的 WBM 方案是在网络管理平台之上叠加一个 Web 服务器，使其成为浏览器用户的网络管理的代理者，网络管理平台通过 SNMP 或 CMIP 与被管设备通信，收集、过滤、处理各种管理信息，维护网络管理平台数据库。WBM 应用通过平台网络管理平台提供的 API 接口获取网络管理信息，维护 WBM 专用数据库。管理人员通过浏览器向 Web 服务器发送 HTTP 请求来实现对网络的监视、调整和控制，Web 服务器通过 CGI 调用相应的 WBM 应用，WBM 应用把管理信息转换为 HTML 形式返还给 Web 服务器，由 Web 服务器响应浏览器的 HTTP 请求。基于代理的解决方案如图 1-130 所示。

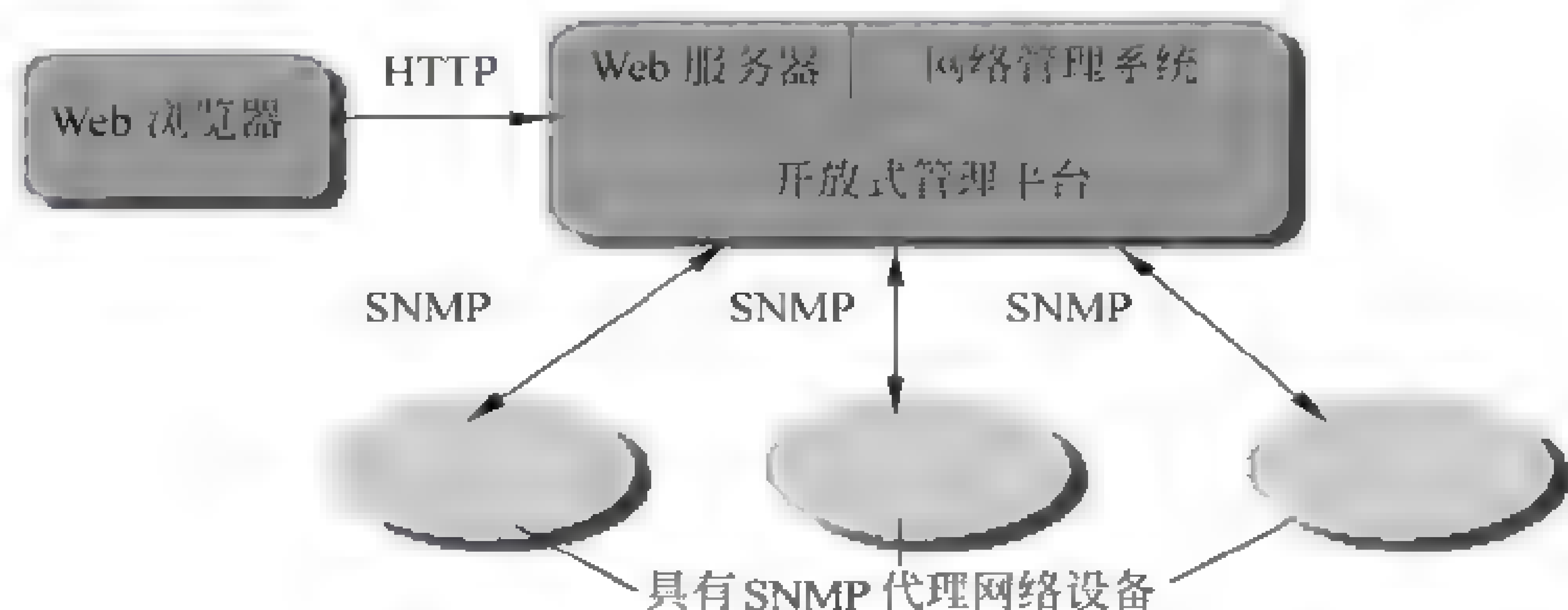


图 1-130　基于代理的解决方案

基于代理的 WBM 方案在保留了现存的网络管理系统的特征的基础上，提供了操作网络管理系统的灵活性。代理者能与所有被管设备通信，Web 用户也就可以通过代理者实现对所有被管设备的访问。代理者与被管设备之间的通信沿用 SNMP 和 CMIP，因此可以利用传统的网络管理设备实现这种方案。

2）嵌入式 WBM 解决方案

嵌入式 WBM 方案是将 Web 能力嵌入到被管设备之中。每个设备都有自己的 Web 地址，使得管理人员可以通过浏览器和 HTTP 协议直接进行访问和管理。代理的解决方案继承了当今传统的基于工作站的管理系统和产品的所有优点，此外它还具有访问灵活的特点。因为代理服务器和所有的网络终端设备通信仍然通过 SNMP 协议，因而这种解决方法可以和只支持 SNMP 协议的设备协同工作。从另一方面来看，内嵌服务器的方法带来了单独设备的图形化管理。它提供了比命令行和基于菜单的 Telnet 接口更简单易用的接口，能够在不牺牲功能的前提下简化操作。嵌入式 WBM 方案如图 1-131 所示。

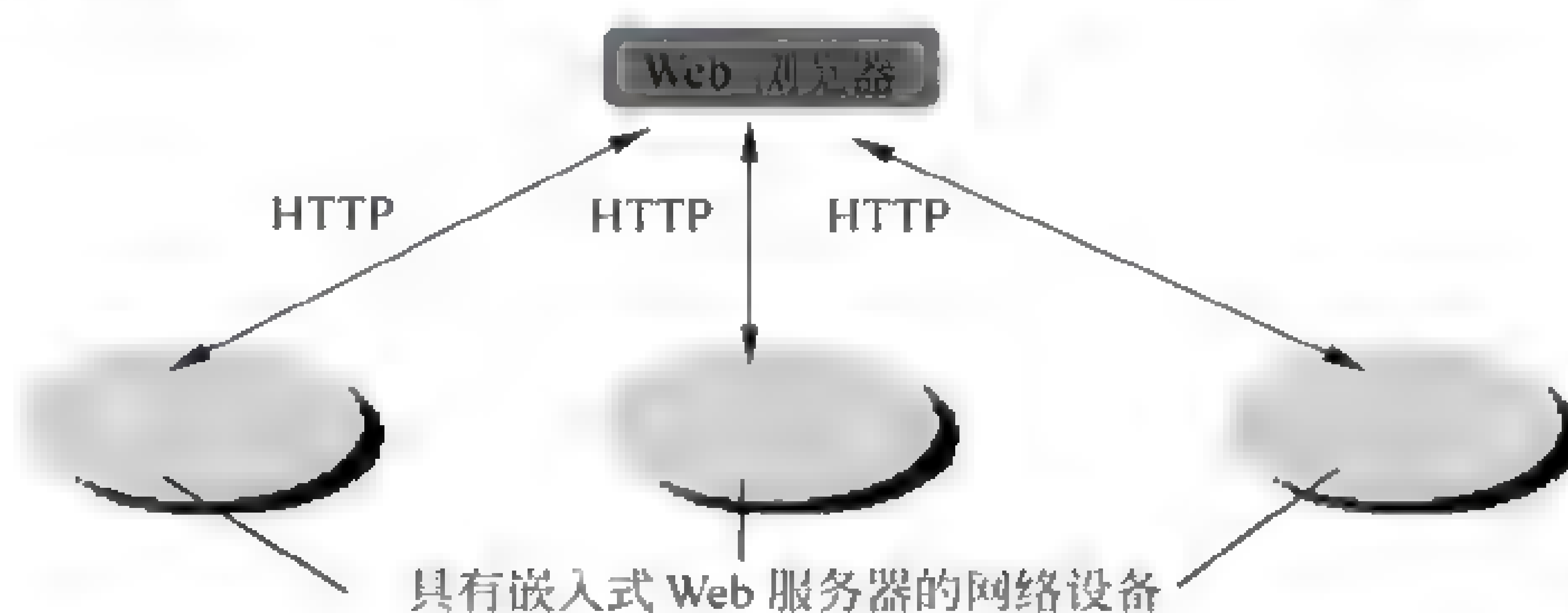


图 1-131　嵌入式 WBM 解决方案

嵌入式方案给各个被管设备带来了图形化的管理，提供了简单的管理接口。网络管理系统完全采用 Web 技术，如通信协议采用 HTTP 协议，管理信息库利用 HTML 语言描述，网络的拓扑算法采用高效的 Web 搜索、查询点索引技术，网络管理层次和域的组织采用灵活的虚拟形式，不再受限于地理位置等因素。

在今后的企业网络中，基于代理服务器和内嵌 Web 服务器的方案肯定会更广泛被用来管理网络，大型的企业将继续需要使用基于代理服务器的管理方案实现对整个企业网络的监控和管理，而内嵌式 Web 服务器的管理方式由于提供了高度改良的接口，因而使企业网络安装和管理新设备时更加方便。

内嵌 Web 服务器的方式对于小型办公室网络来说是理想的管理方式。小型办公室网络相对来说比较简单，也不需要强大的管理系统和整个企业的网络视图。由于小型办公室网络经常缺乏网络管理和设备控制人员，而内嵌 Web 服务器的管理方式就把用户从复杂的管理中解脱出来。另外，基于 Web 的设备实现了真正的即插即用，减少了安装时间和故障排除时间。

实现 WBM 的技术有多种，最常用的是描述 WWW 页面超文本标记语言——HTML。HTML 可以构建页面的显示和播放信息，并可以提供对其他页面的超级链接，图形和动态元素（如 Java Applet）也可以嵌入到 HTML 页面中。因此用 HTML 页面提供 WBM 的用户信息接口是很理想的。

另一项在 WBM 中应用的技术是 CGI，它提供基于 Web 的数据库访问能力。当 WBM 应用程序需要访问 MIB 时，可以利用 CGI 对数据库进行查询，并格式化 HTML 页面。

对 WBM 来说，最重要的技术是 Java 语言。它是一种解释性程序语言，也就是在程序运行时，代码才被处理器程序解释。解释性语言易于移植到其他处理器上。Java 的解释器是一个被称为 Java 虚拟机（JVM）的设备，它可以应用于千变万化的处理器环境之中，而且可以被绑定在 Web 浏览器上，使浏览器能够执行 Java 代码。

Java 提供了一套独立而完备的小应用程序 Applet 专用于 Web。Applet 能够被传送到浏览器，并且在浏览器的本地机上运行。Applet 具有浏览器强制安全机制，可以对本地系统资源和网络资源的访问进行安全控制。Java Applet 对于 WBM 中的动态数据处理是一种有效的技术。它能够方便地显示网络运行的画面、交换机状态面板等图片，也能实时表示从轮询和陷阱得到的更新信息。Java 在 WBM 中还有一种应用就是将 JVM 嵌入到一个设备之中，该设备就可以执行 Java 代码。利用这一点，可以将应用程序代码在工作站和网络设备之间动态地传递。

3．WBM 的安全性

WBM 中的安全性考虑对于企业网络的安全是至关重要的。一个安全的网络需要有防火墙将其与 Internet 隔离开，以保护企业内部网络的资源，比如防止未经许可的对 Web 服务器的外部访问。另外，出于安全考虑，对服务器的访问可以通过口令和地址过滤来控制。从某种角度来看，WBM 也是一个基于服务器的需要保护的设备。由于 WBM 控制着网络的主要资源，因而只有 Intranet 上的授权用户才能访问 WBM 系统。基于 Web 的设备在向用户提供易于访问的特性的同时，也可以限制用户的访问。管理员可以对 Web 服务器加以设置以使用户必须用口令来登录。WBM 方式并不和业已存在的安全性方式相冲突，如已经在 Windows 和 UNIX 操作系统中应用的目录结构、文件名结构等。另外管理员还可以很方便地使用复杂的鉴定技术来加强 WBM 系统的安全。

网络管理人员的操作数据是非常敏感的，如果在浏览器到服务器之间的传输过程中被侦听或篡改，会造成严重的安全问题。因此这些数据在传输过程中通常需要加密。这个需求利用现有的技术是可以满足的，因为基于 Web 的电子商务同样需要数据传输的安全，这种技术已经得到了大力开发，并取得了成功。

此外，Java Applet 的安全问题对 WBM 也很重要。因为 Java Applet 将字符串和数据暴露在光天化日之下，因此存在着被篡改的危险。尽管 Java Applet 具有一些安全保障，如被规定不能写盘、破坏系统内存或生成至非法站点的超级连接。但仍需要对代码进行保护，以保证收到的 Applet 与原有代码完全相同。目前这项技术已基本成熟。

为了降低网络管理的复杂性、减少网络管理的成本，WBM 管理的开放式标准必不可少。有两个 WBM 的标准目前正在考虑之中：一个是 WBEM（Web-Based Enterprise Management）标准，另一个是 JMAPI（Java-Management Application Program Interface）标准，现在发展成 JMX（Java Management Extension）。

1.9.4.2 典型网络管理工具

网络管理系统提供了一组进行网络管理的工具，网络管理员对网络的管理水平在很大程度上依赖于这组工具的能力。网络管理软件可以位于主机中，也可以位于传输设备内（如交换机、路由器、防火墙等）。网络管理系统应具备 OSI 网络管理标准中定义的网络管理五大功能，并提供图形化的用户界面。

针对网络管理的需求，许多厂商开发了自己的网络管理产品，并有一些产品形成了一定的规模，占有了大部分的市场。它们采用了标准的网络管理协议，提供了通用的解决方案，形成了一个网络管理系统平台，网络设备生产厂商在这些平台的基础上又提供了各种管理工具。下面我们将简单介绍一些具有较高性能和市场占有率的典型网络管理工具。

1. CiscoWorks for Windows

CiscoWorks for Windows 是一个全面的基于 Web 的网络管理解决方案，它主要应用于中小型的企业网络。它提供了一套功能强大、价格低廉且易于使用的监控和配置工具，用于管理 Cisco 的交换机、路由器、集线器、防火墙和访问服务器等设备。使用 Ipswitch 公司的 WhatsUp Gold 工具还可管理网络打印机、工作站、服务器和其他重要的网络设备。

CiscoWorks for Windows 中包含以下组件：

1）CiscoView

CiscoView 提供图形化的前后面板的视图，能够以各种颜色动态地显示设备的状态，并提供对某一特定设备组件的诊断和配置功能。CiscoView 可以从 CiscoWorks for Windows Desktop 或 WhatsUp Gold 下启动。如果是从 CiscoWorks for Windows Desktop 下启动，可以从设备列表中选择要监视的设备。如果要监视的设备不在设备列表中，则直接输入设备 IP 地址。选择了一个设备之后，将出现有关该设备信息的页面，如图 1-132 所示。如果想从 WhatsUp Gold 下启动 CiscoView，在 Network Map 下选择要监视的设备，然后单击右键，选择 CiscoView 菜单项，同样会出现如图 1-132 所示的页面。

2）WhatsUp Gold

WhatsUp Gold 是一种基于简单网络管理协议（SNMP）的图形化网络管理工具，可以通过自动或手工创建网络拓扑结构图管理整个企业内部网络，支持监视多个设备，具有网络搜索、拓扑发现、性能监测和警报追踪的功能，如图 1-133 所示。



图 1-132　CiscoView 界面

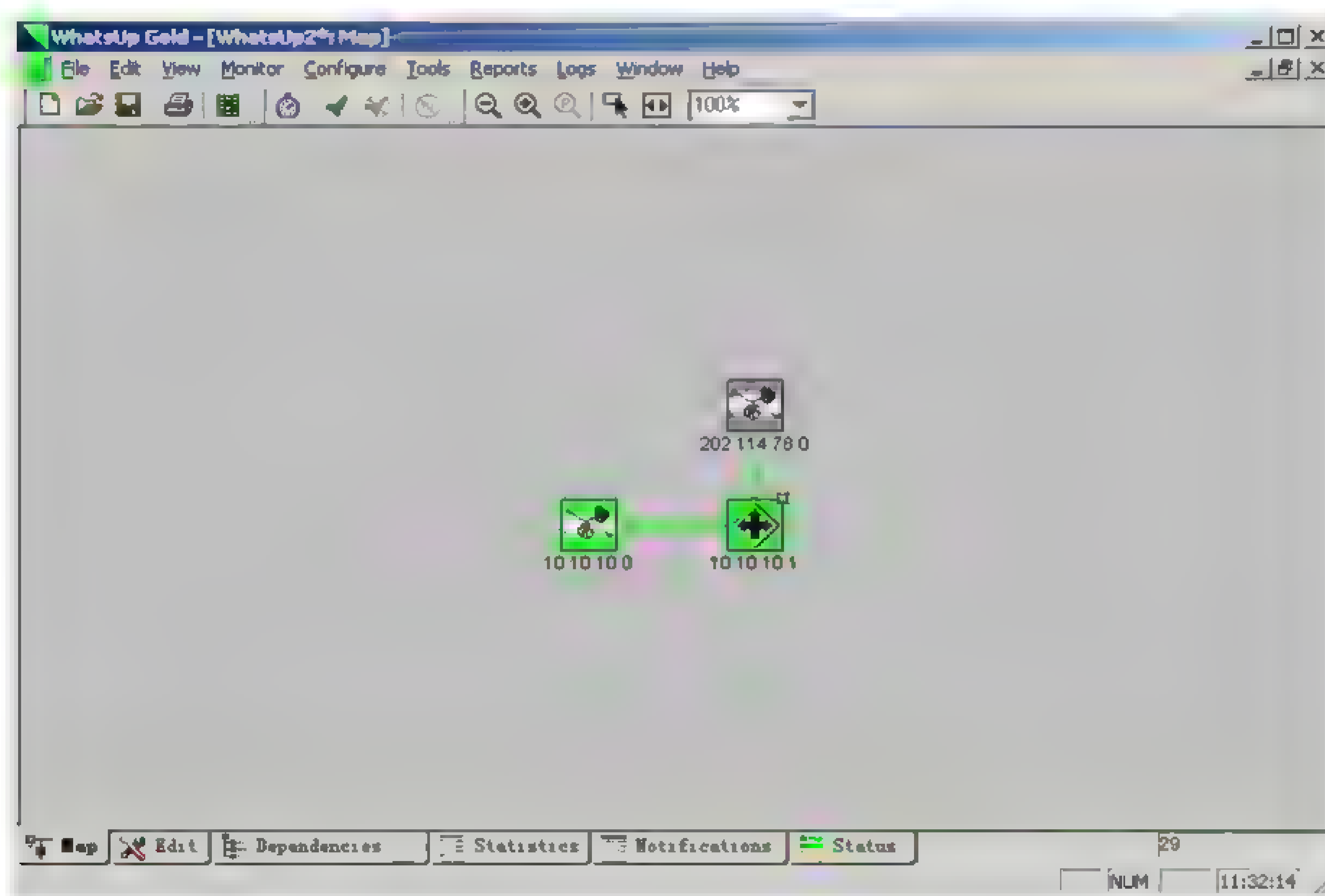


图 1-133　WhatsUp Gold 用户界面

3）Threshold Manager

Threshold Manager 使用户能够在支持 RMON 的 Cisco 设备上设置极限值及获取事件信息，以降低网络管理费用，增强发现并解决网络故障的能力。使用 Threshold Manager 之前，必须建立 Threshold Manager 模板。Cisco 公司提供了一些预定义的模板，用户也可以自行定义自己的模板。Threshold Manager 具有以下功能：

- 支持实现 RMON 事件和警报组的 Cisco 设备。

- 给某个 MIB 变量设置阈值。
- 为某个设备的多个接口设置阈值。Threshold Manager 能够自动区分接口的不同类型和速度，并为接口设置适当的阈值。
- 自动地应用已定义的 Threshold 模板。
- 事件日志管理，并为用户提供某个事件的详细信息。

当超出为某个设备设置的阈值时，就发生了一个事件，然后设备中的代理就会执行下列功能：首先是产生一个警报，然后该事件记入日志，并向一个或多个网络管理站点发送一个陷阱（trap），接着 Threshold Manager 将执行下列功能：显示刚刚记录在日志里的事件，将事件与 Threshold 模板关联起来，之后，管理员可以通过检查这些事件来发现潜在的问题。Threshold Manager 管理界面如图 1-134 所示。



图 1-134 Threshold Manager 管理界面

在图 1-134 中，Event Log 窗口以表格的方式显示越界事件信息，并以 RMON 日志记录存在被管理的设备上；Device Threshold 窗口用来显示、设置当前被管理设备的系统或接口的阈值；Templates 窗口用来显示所有默认的或用户定制的模板，也可以建立新的模板；Trap Receivers 窗口可以用来增加或删除接收陷入事件的管理站点；Preferences 窗口可以用来设置 Threshold Manager 的属性。

4）Show Commands

Show Commands 使用户不必记住每个设备复杂的命令行语法，通过使用 Web 浏览器进行简单操作就可以获得有关设备详细的系统和协议信息。Show Commands 在 Web

页面的左边以树型显示了某设备所支持的命令列表，如图 1-135 所示。当用户选择了一个命令后，Show Commands 将执行下列功能：

- 在设备上执行所选择的命令。
- 从设备上搜集输出信息（包括系统和协议信息）。
- 在屏幕上显示输出信息。

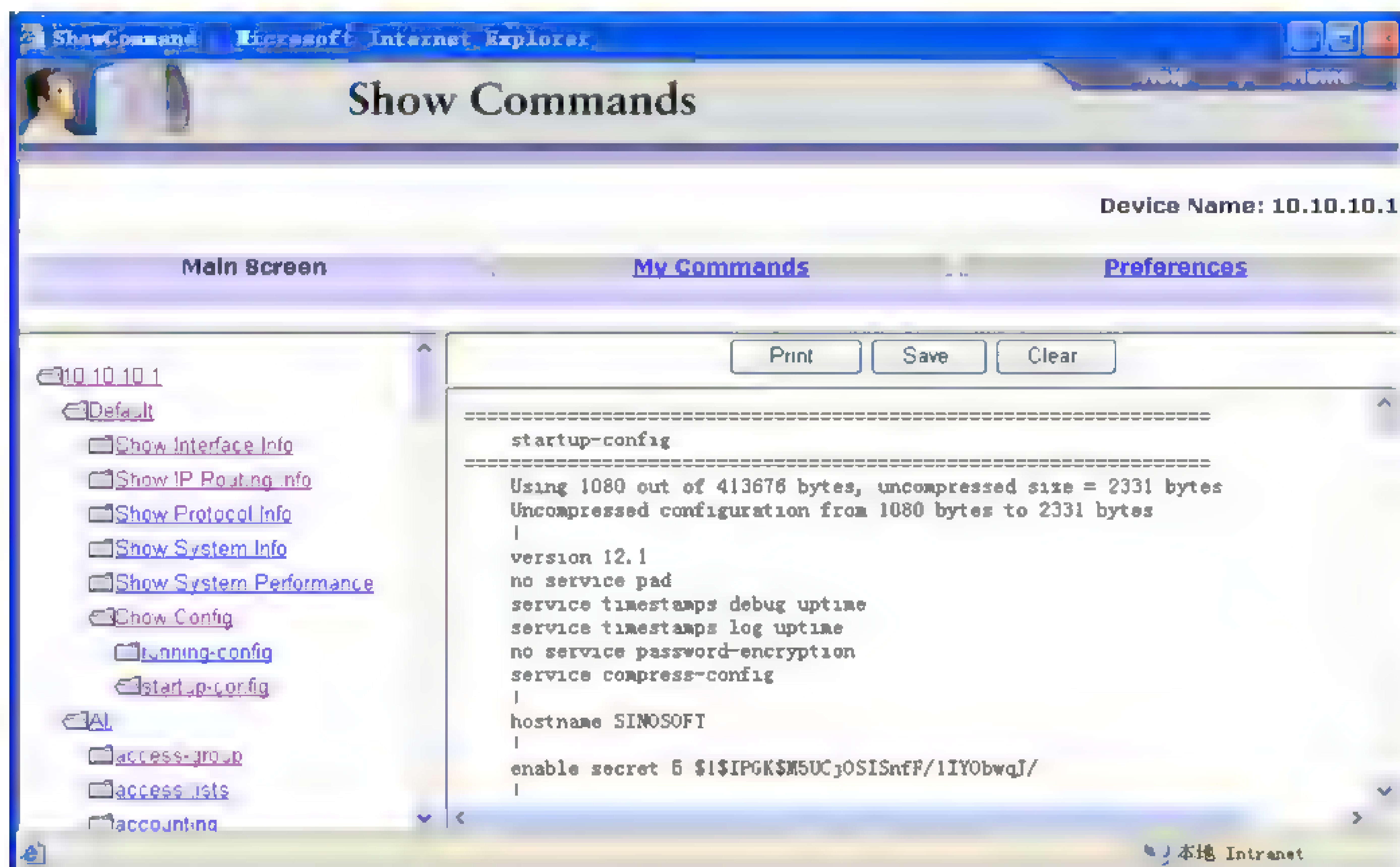


图 1-135　Show Commands 操作界面

2．HP OpenView

HP OpenView 作为强大的网络和系统管理工具，可以帮助企业主动地实现系统和网络管理。其中，HP OpenView 应用和系统管理解决方案（Integrated IT Management Solution）是企业集成化管理解决方案的基本组成部分，它以服务质量战略为核心，利用针对业务应用管理的新技术，为企业提供最全面的 IT 系统和应用管理。

企业各项业务的日益电子化，IT 部门的职责是否能够成功实现由内向外的转变（为外部客户提供高性能、高可用性、安全的 IT 服务），已经成为一个迫在眉睫的问题。HP OpenView 是一项具有战略性意义的产品，它集成了网络管理和系统管理各自的优点，并把它们有机地结合在一起，形成一个单一而完整的管理系统，从而使企业在迅猛发展的 Internet 时代取得辉煌成功，立于不败之地。

HP OpenView 应用和系统管理由多个功能套件组成，针对不同的需求，完成不同的管理功能。HP OpenView 包括以下功能套件。

- 一体化网络和系统管理平台：HP OpenView Operations。
- 功能强大的报告管理：HP OpenView Reporter。
- 端到端资源和性能管理：HP OpenView Performance。
- 具有实时诊断和监控功能的：HP OpenView GlancePlus。
- 提供可全面管理系统可用性与性能的综合性产品：GlancePlus Pak 2000。
- 对服务器与数据库的性能和可用性进行管理的 HP OpenView Database Pak 2000。

这些模块相互依存，相互支持，集成为功能强大的系统和应用管理平台，为企业提供最全面的集成化应用和系统管理功能。以下将对上述功能套件作一些简单的介绍。

HP OpenView Operations for Windows 管理服务器能支持数百个受控节点和数千个事件。它不仅可以通过服务视图来扩展企业的传统运营管理，还可以从任意地点进行跨平台电子商务基础设施的管理。借助它，企业可从服务角度进行管理、管理混合电子商务基础设施并获得在基本运行管理基础上创新的能力。

HP OpenView Operations for UNIX 是由业务驱动的管理模式，它使企业快速控制电子化服务。作为分布式大型管理解决方案，它能监视、控制和报告 IT 环境的状态，实现深入的超大型混合管理，延长组成电子企业环境的各个部件的正常运行时间。正是因为该管理模块具有如此强大功能，运用它复杂的 IT 系统进行管理，使系统拥有了高效性、实用性、可扩展性特点，提高工作效率，减少资源和成本的浪费，保障了各业务系统平稳、健康地运行。

HP OpenView Reporter 模块为企业分布式的 IT 环境提供的廉价、灵活、易用的管理报告解决方案。它提供了标准和可定制报告，自动将 HP OpenView 在所有支持平台上获取的数据转化为企业可利用的重要管理信息。Reporter 使报告能经由 Web 浏览器发布，企业中能访问 Web 浏览器的每个人都可立即获得报告。并无缝地集成在 HP OpenView 系列之中，使企业根据所收集的数据提供集成化的中央管理报告解决方案。

HP OpenView Performance 是一种强大的端到端资源和性能管理组件。无论管理环境是由单一系统构成还是由大型系统网络构成，它都能收集、总结和记录来自应用、数据库、网络和操作系统的资源和性能测量数据，并把这些数据进行整理后转为对用户有用的信息，最终以经济有效的方式为用户提供最佳的服务级别；HP OpenView Performance 可深入检查资源使用率和性能趋势，通过这一信息，管理人员可以发现系统瓶颈。通过比较活动水平，可均衡工作负载，提供保持系统平滑运行的信息，使用户可以有效地控制和利用资源，及时调整多个分布式的系统环境，对系统中影响服务层和用户层的故障做出响应；同时还使系统管理员能有效扩展其管理范围，对本地和远地的系统进行有效管理和监控，此外，HP OpenView Performance 数据可以多种格式输出，用于容量规划、统计数据分析和电子数据表应用中。从而在性能管理和问题分析、资源规划和服务管理等主要领域满足企业的分布式管理要求。

HP OpenView Database Pak 2000 管理模块，对服务器与数据库的性能和可用性进行

管理。它提供强大的系统性能与诊断功能；有效收集并记录系统与数据库统计数据并进行告警；能够检测关键事件并采取修复措施；提供200多种测量数据和300多种日志文件状态。利用安装在服务器上的Database Pak 2000，用户可以及时地发现数据库与系统资源的性能问题，以防止进一步恶化，及时有效地对系统和数据库进行管理。

以上模块既相对独立，又可完全集成在一起，为企业提供高可用性的系统管理解决方案。例如，HP OpenView Operations可以与Network Node Manager、Reporter及Performance等结合在一起，完全集成于HP OpenView系列之中，共同构成HP OpenView解决方案的中央控制台，对IT系统提供全面的管理。正是由于HP OpenView应用和系统管理解决方案拥有如此强大的集成功能，并且适合不同规模的企业使用。而中小企业的崛起和普及，为HP OpenView的应用提供了更大的发展空间。

3．IBM Tivoli NetView

Tivoli NetView是IBM公司著名的网络管理工具，能够提供整个网络环境的完整视图，实现网络产品的管理。它采用标准的SNMP协议对网络上符合该协议的设备进行实时的监控，对网络中发生的故障进行报警，从而减少系统管理的管理难度和管理工作量。NetView以其先进性、可靠性、安全性获得业界好评，在市场上具有较高的占有率。

通过IBM Tivoli网络管理解决方案，可以实现的功能主要包括以下一些。

1）网络拓扑管理

自动发现和生成网络拓扑是网管软件的基本功能要求。Tivoli NetView能够自动发现联网的所有IP节点，包括路由器、交换机、服务器、PC等，并自动生成拓扑连接。NetView提供按照网络节点所在的地理位置对网络拓扑图进行客户化，使之与实际的网络结构更加吻合。图1-136是Tivoli网络管理拓扑显示界面。

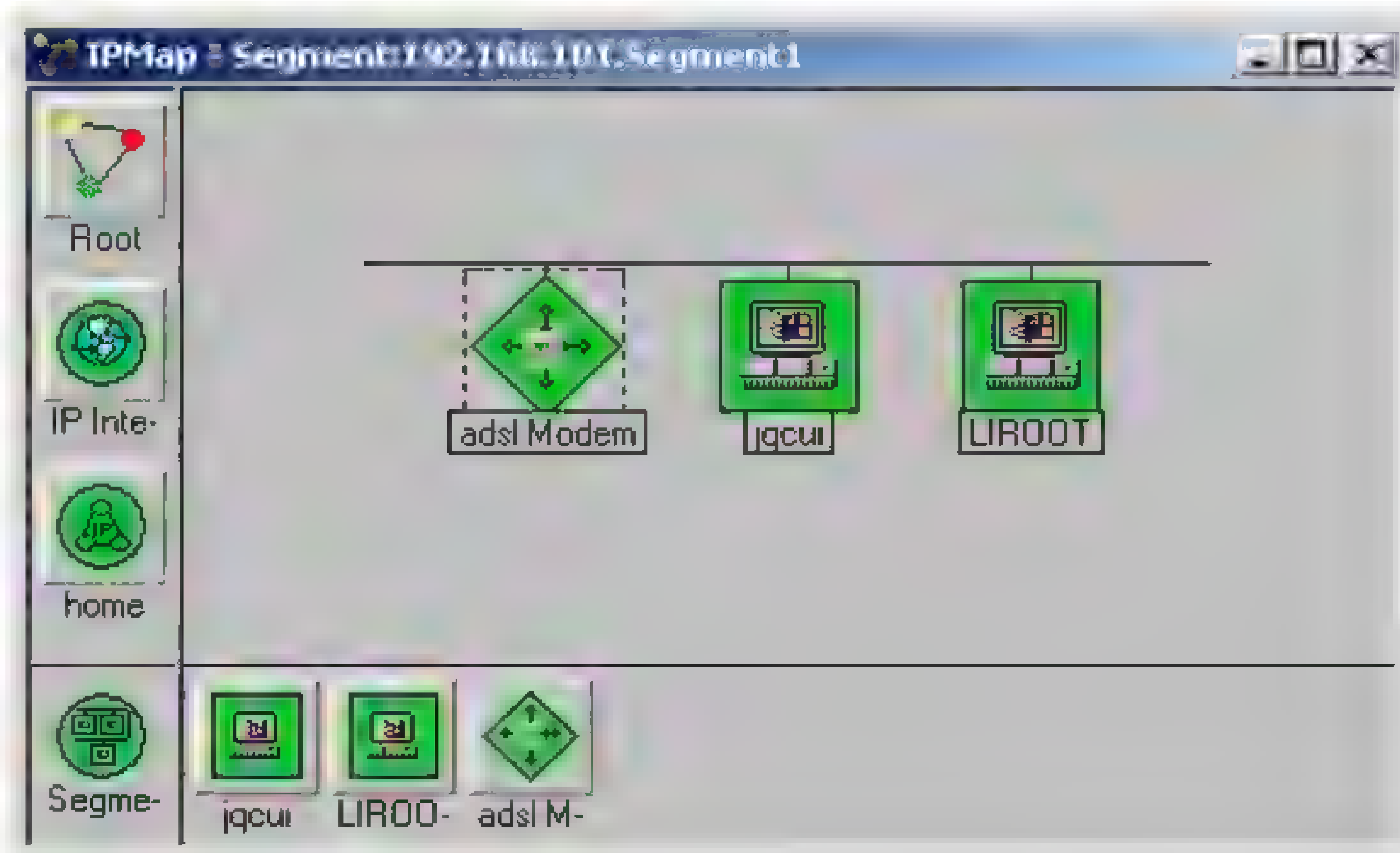


图1-136　Tivoli 网络管理拓扑显示界面

NetView 提供 SmartSet 的功能，能够将具有相同属性的重要管理对象做成管理集合，例如，用户可以把重要的路由器放在一起作为一个 SmartSet，以方便对这些路由器作统一的管理设置。与其他信息收集工具不同，Tivoli NetView SmartSet 不需要手工加入对象，管理员只需设置加入的属性条件（如条件为 Cisco 路由器），SmartSet 能够动态发现符合该条件的设备并自动加入，因而消除了人为错误和过时信息，为管理员提供了很大的管理便利。

2）网络故障管理

网络故障管理是网络管理的核心，网管软件应当能够及时发现网络的故障，按照故障的轻重缓急产生不同的报警，并且具备对故障事件自动处理的能力。Tivoli NetView 图形化的网络 IP 拓扑结构，使网络管理员可以迅速方便地发现区域网上出现故障的 IP 资源并帮助管理员分析故障原因。当网络中的设备出现故障，机器死机或网络链路中断，NetView 会及时在屏幕上出现报警信号，并在拓扑图中将该设备置成红色。便于网络管理人员发现诊断。

3）网络性能管理

网管人员需要了解网络实时的性能状况，需要能够对网络性能作出分析和预测，并生成相应的报表。Tivoli NetView 的 SnmpCollect 功能，能够自动采集重要的网络性能数据，如 IP 流量、带宽利用率、出错包数量、丢弃包数量、snmp 流量等，并设置相应的阈值，当所采集的数据达到阈值时能够触发报警或者定义好的自动操作。可以用图形的方式显示这些网络性能数据的变化情况，也可以将这些数据存放于关系型数据库系统中，以便于检索和分析，如图 1-137 所示。

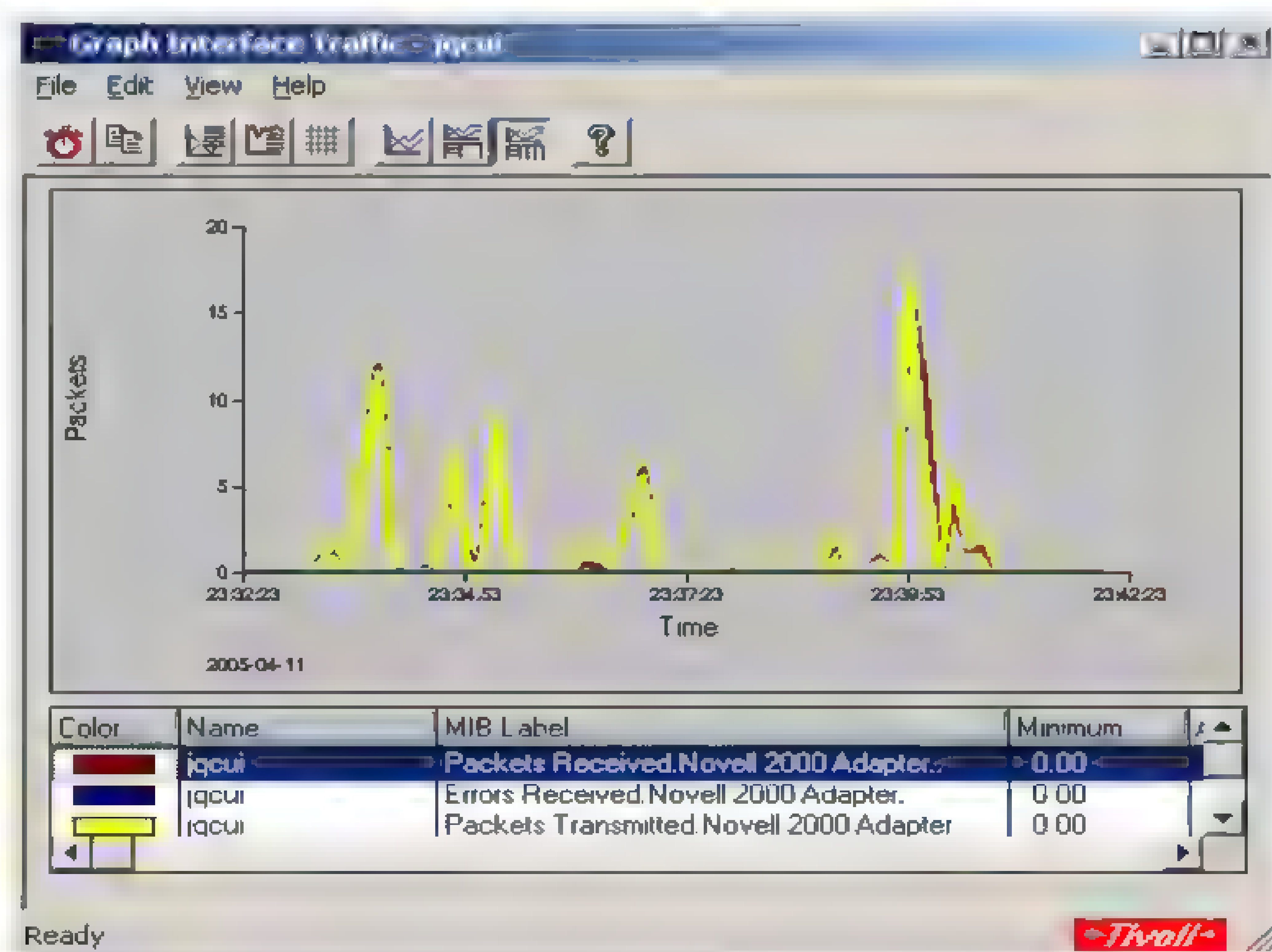


图 1-137 网络性能分析监控显示

Tivoli Data Warehouse 将为网络性能管理提供集中的历史统计和报表分析，能够帮助管理人员从大量数据中及时发掘出可以用作判断网络运行状况的数据，能够生成各种报表和图形化的分析报告。

4）网络设备管理

Tivoli NetView 是使用最广泛的网络管理平台之一，支持业界标准的 API，能够与主要网络设备厂商的设备管理软件，如 CiscoWorks、Nortel（Bay）Optivity、3com Transcend 等方便地进行集成，从而能够统一从 NetView 的 Console 对各种网络设备进行监控和配置。

通过使用 Tivoli NetView 与网络设备管理软件的集成，管理人员可以全面地管理网络、网络设备、网络性能，及时获取网络故障的信息，从而在最短时间内解决网络故障。

5）管理权限分配

Tivoli NetView 可以为管理员定义不同的管理角色，不同的管理员可以被授权管理不同地址范围的设备，而且没有权限管理的设备不会在拓扑图中显示出来。

6）Web 管理功能

Tivoli NetView 通过 Web Console 实现分布式管理界面。NetView Web Console 为用户提供了一个灵活、可配置的环境，以便用户可以访问网络状态和配置信息。

使用 Web Console 可以浏览交换机的端口状态、路由器状态、MAC 地址状态等，方便了交换机管理。

7）支持 MPLS 管理功能

NetView 7.1 支持对 MPLS 设备的识别，并能对有关 MPLS 的数据进行查询。NetView 可以管理 LSR（Label Switch Routers）设备。

8）交换机的故障定位

IBM Tivoli Switch Analyzer 提供第二层交换设备发现功能，识别包括第二层和第三层交换设备在内的设备之间的关系。正确的关联分析，无论其根源是一个 IP 寻址的端口还是一个第二层的局域网（LAN）交换机上非 IP 寻址的端口、板卡或插件。另外，IBM Tivoli Switch Analyzer 还扩展了 IBM Tivoli NetView 和 IBM Tivoli Enterprise Console 的故障根源分析功能。

9）整合和关联

通过提供第二层发现功能以及第三层拓扑结构的关联，Tivoli Switch Analyzer 能够在不需人员干涉的情况下生成一个故障根源解决方案。

10）自动化管理

IBM Tivoli Switch Analyzer 能够通过第二层交换设备的 SNMP 信号自动地发现第二层交换机设备和识别网络关系。运用该信息，Tivoli Switch Analyzer 能够掌握识别的交换机、端口、板卡和插件与已知的第三层拓扑的关系。Tivoli Switch Analyzer 把从第二层交换设备得到的信息与第三层的信息相混合，用来帮助形成一个第二层和第三层交换拓扑结构的更完整的视图。

11）冗余路径相关

IBM Tivoli Switch Analyzer 支持网络中的冗余结构，这需要为故障根源的关联而做出特殊的考虑。网络的星型和网状结构可能导致毫无意义的上行或下行传输冲突，这意味着在这些复杂的环境中应该有附加的逻辑来使其进行关联处理。Tivoli Switch Analyzer 用业界独特的第二层故障根源关联处理解决了这个问题，它主要是考虑了底层接口、端口和插件的逻辑负载。

12）安全性、核查和控制

Tivoli Switch Analyzer 运用操作系统软件和 Tivoli 管理框架的安全和核查功能来防止入侵，访问核查跟踪记录并进行分级。

4. Sun Net Manager

随着客户机/服务器计算技术的爆发性增长，如今的企业面临着如何最好地管理复杂的、异构的环境。这个挑战由于没有一致的管理平台管理不同大小的环境而变得更加复杂。低档平台可以经济有效地管理小的网络，但是不能调整到管理大的环境。相反地，高档企业管理平台由于价格较高不适于小的网络。此外，平台一般没有提供平台之间的允许跨网络管理的分布产品。为了满足这个需要，Sun 公司开发了 Solstice Site Manager 和 Solstice Domain Manager，它们均是基于 Sun Net Manager 和 Cooperative Console 技术的网络管理产品。

Sun Net Manager 的分布式结构和协同式管理独树一帜。Sun Net Manager 具有如下特点。

1）分布式管理

Sun 采取分布式管理，有三种管理模式：外部到中央的管理系统可以在必要时接管外部点的网管；分级的管理方式可以缩小网管的容量，必要时还可以相互接管；协同的管理方式，两个 Domain Manager 的数据库可以保持同步，必要时可以互相接管工作。

与 Sun Net Manager 通过 RPC 沟通的 Agent 有两种类型：直接存取管理对象，如 CPU 统计 Agent、磁盘信息 Agent 等；非直接存取规律对象，也称 Proxy Agent（委托代理）。

Proxy Agent 是分布式管理体系结构的基础，它可以很容易地扩充网管容量。规模化的管理用 Proxy Agent 来实现。这种 Proxy Agent 为用户带来三方面的好处：网络管理的轮询（polling）局部化，减少了文件传输的开销，增加了每个管理者可管理的节点数；Proxy Agent 为远程 Agent 提供了广域网上可靠的传输；通过提供不同类型的 Proxy Agent，可使 Sun Net Manager 管理任何类型协议的对象，例如 DECnet 网和 FDDI 网等。

Sun Net Manager Agent 和 Proxy Agent 与应用程序通过 RPC（ONC/RPC）协议进行通信。Proxy Agent 将 RPC 协议翻译成被管理元素所能理解的协议，通过它，Sun Net Manager 可以管理小量的资源，包括：通信协议层和接口；网络设备如交换机、路由器、集线器、打印机、工作站和 PC；应用程序、数据和网络服务；系统和操作系统资源。

2）协同管理

协同管理是由 Sun Net Manager 和 Cooperative Console 共同实现的，其主要特点是信息的分布采集、信息的分布执行、应用的分布执行。我们可将一个小型企业网管按其业务组织或地域分为若干区，每个区都有自己独立的网管系统。但有关区之间可以互相作用。区与区之间的关系可根据实际需要灵活配置，既可以层次，也可以为对等，甚至可以根据被管目标的特性管理职能，例如路由器、X.25 服务器、数据库应用等可分别由不同区域的网管中心来管理，从而充分发挥各地技术专家的特长。

Sun Net Manager 2.3 不但提供了易用的生成事件请求的工具，而且还提供了非常好的事件管理功能来监视关键设备的状况。Sun Net Manager 2.3 引进了一个新的特性：基于事件的动作（event-based actions）。一个预先定义的事件发生，可激发一个接着发生的事件请求。管理者可以将多个预先定义的请求连接起来，以快速诊断问题所在。

Sun Net Manager 2.3 还允许对某一类设备（如 Cisco 路由器）提交一个共同的事件请求。

3）全面支持 SNMP

简单网络管理协议是一个用于管理信息交换的工业标准。Sun Net Manager 包括了所有基本的 SNMP 机制，而且允许配置 SNMP 陷阱（trap）为不同的优先等级。在网络中出现故障时，能够传送到其他 Solstice 或非 Solstice 的平台上，如需要对 IBM 的小型机实现一体化的管理，Sun 公司相应的解决方案实现 SNMP 陷阱到 IBM Netview 的传送。Sun Net Manager 同时还支持 SNMP v2。

4）具有较强的安全性

在分布式网管系统中，网络管理系统的安全性显得特别重要，在配置 Cooperative Console 时，系统提供访问控制表以保证具有那些被授权接受管理数据的人才能得到相关信息。另外 Cooperative Console 还提供了只读控制台的功能，使得一般的网管人员只能在只读方式下操作，不能增加/移动/删除网络元素。

5）用户工具

Sun Net Manager 的用户工具很丰富，它可使操作员监视和控制网络及系统资源。图形化的界面简化了操作过程和减轻了培训要求，这些工具主要包括以下一些：

- 管理控制台（management console）。
- 搜寻工具（discover tool）。
- Solstice Domain Manager 版面排列工具。
- IPX 搜寻工具（IPX discover）。
- 浏览工具（browser tool）。
- 图形工具。

6）应用程序接口

Sun Net Manager 既提供了用户工具，又提供了开发者工具。开发者工具是三个应用编程接口（API），厂商和用户可基于 API 开发更强大、更具个性化的工具，以扩展 Sun

Net Manager 中用户工具的功能。这三个 API 分别是：管理者服务 API（manager services API）、代理服务 API（agent services API）和数据库/拓扑图 API（database/topology map services API）。

1.9.4.3 网络管理应用

所谓的“网络和系统管理”，究竟应该管理哪些内容呢？对于不同的人，网络和系统管理有着不同的含义。对于一个简单的网络环境，如办公局域网来说，用网络分析工具监控一个孤立的网络也许就能满足要求。对于企业级的大型网络，也可能是涉及分布式数据库、网络设备的自动轮询、网络拓扑管理的大型分布式系统。此时的网络和系统管理就是要利用各种手段帮助管理人员监控和维护所有的 IT 资源，包括网络设备、服务器、数据库等。具体表现为如下几个方面：

（1）端到端的系统监控管理。

（2）减少系统故障时间。

（3）使系统发挥最大的性能。

（4）实现最大程度的自动化操作。

（5）保障企业系统安全。

（6）保障业务系统平滑地运行。

（7）规范业务支持流程。

（8）IT 系统更好地为客户服务。

例如，对于一个将数据存放在不同地方的公司，其差别可能表现在设备不同，如存放在不同的 PC、工作站、服务器或专用计算机上；部门不同，如可以在计算中心，也可以在其他各个部门；网络不同，如可以在内联网上，也可以在外部供货商和经销商的网络中。其网络设备组成也会表现为体系结构不同或使用多厂商的设备，对于这样的情况，可以从以下几个方面考虑问题。

（1）数据集成。系统应该有统一的文件系统结构和数据访问控制规则，可以通过防火墙等安全设备来划分各自独立的文件系统和数据库，也可以通过本地透明访问来创建全球虚拟化。

（2）透明性。需要有与命名相关的统一命名空间，使用户可以利用一条访问路径找到他们所需要的信息，而不用关系他们碰巧使用了哪些计算机。

（3）安全性。允许指定各区域任务和安全性的“域”。访问系统必须规定对安全破坏发生时的访问过滤策略、身份验证机制、信息初始化和事件处理。还设计利用备份进行冗余数据存储时保持数据的一致性问题，使用数据备份防止数据临时丢失，以及以归档的方式进行长期数据存储备份。由于一些数据经常存储于不同的位置的不同存储结构层次上，必须定义这些不同层次之间的数据迁移策略。

再如，某个专利办公室的专利检查员需要使用多极检索程序来检索大约 2000 万个图形文件，另外还必须提供对 60 万个文本文件的全文检索。这个时候，依据 SLA，该

系统必须提供可用性为 98%的工作时间；在并行查询的检索次数为 60 次和高达 10 万次命中，响应时间应该小于 3s/查询；显示时间是文档内 0.7s，文档之间 1.5s。

这种情况时，相应的管理任务包括以下一些内容：

（1）根据 SLA 检测服务质量。

（2）应用模块管理。如软件分发、参数提供、搜索系统更新、运行分布式“搜索”应用模块。

（3）网络和系统管理。底层操作（网络和终端系统）的安全性、数据备份。

（4）用户管理、计费管理。

（5）依据服务质量提供报告和详细服务。

市场竞争越来越依赖于信息处理和交换，有时甚至是真实价值和物质的交换，如股票市场、汇款、订货、模拟和虚拟现实，因此，分布式系统的商业处理任务越来越重，其管理的重要性也越来越突出。

由于系统的复杂性、变更的灵活性、服务的可用性以及运行成本等因素，造成了管理上的许多障碍。管理技术、方案、方法的多样性，对管理人员提出更高的要求。

当今的产品和服务必须适应飞速变化的市场。依靠信息处理的商务和生产活动不得不跟上市场的需求。对于管理方案也有灵活性的要求。同时，管理系统还必须具备一定的灵活性，以适应不同层次的管理变化，以及物理位置、软硬件和处理负载等的变化。

分布式系统自身不是目的，它们是用来提供服务的。服务的提供必须依据 SLA。但是，仅仅从功能的角度描述服务是不够的。需要有一个可操作的接口来调用和评价服务。这里的评价意味着能对所达到的服务质量进行评价。QoS 对服务质量、服务安全质量和客户服务质量从整体上进行评价，是服务提供商和服务用户之间的典型接口信息。

尽管网络管理的解决方案针对不同层次的应用需求有着具体细节上的不同，但是网络管理的基本应用还是由以下几个方面构成：网络资源状态监视、阈值监视、事件管理、配置应用、拓扑管理以及性能监视等。

（1）网络资源状态监视。

监测资源的目的在于尽可能获得有关资源服务质量和状态的最新信息。监测涉及到访问某些资源的属性，监测总是由管理工作站发起的，管理工作站轮询资源并分析轮询结果。因此，实现监测功能极大地依赖于对单个资源进行寻址所采用的协议。

（2）阈值监测。

阈值的设定在很大程度上取决于设计者的经验知识，目前还没有哪种工具能够支持对监测过程进行切合实际的阈值配置。阈值主要是通过管理工作站进行指定、管理和监测、当网络管理系统检测到超出阈值的情况时，就向事件管理应用程序发出相应的事件。

（3）事件管理。

事件管理负责接收和处理事件，这些事件可以由被管设备产生并发送给管理工作站的外部事件，也可以是由网络管理平台的其他部件，比如阈值监测过程所产生的内部

事件。

事件对用户的可视化是一种重要的功能。可视化建立在被管资源的状态模型的基础上，这样一种模型描述了资源的状态与导致状态变化的事件之间的关系。

（4）配置应用。

配置应用向用户提供了对资源的写访问，配置应用可以分成如下几种形式：

- 有关当前资源配置的信息。可使用 SNMP 询问诸如路由表、接口表、地址表和 ARP 表等。
- 通过管理协议改变配置。SNMP 协议的 Set 服务用来改变部件中的配置信息。这里的难点之一是，由于 SNMP 的安全问题，许多厂商并不允许对资源的写访问。
- 通过登录系统进行配置。设备制造商提供允许用户登录系统直接改变系统配置的工具，当使用网络管理平台时，用户可以通过图形用户界面直接登录系统，比如使用 Telnet。

（5）拓扑管理。

网络管理平台的另一种重要功能是拓扑发现功能。它是使用管理协议收集尽可能多的有关网络的资源的配置信息，并且保存在网络管理平台的数据库中。

（6）性能监视。

性能监视用于定义和执行性能测量，与阈值监视类似，测量由以下参数定义：

- 通过指定系统和被测量的属性来选择测量点。
- 选择测量间隔，即选择执行测量的采样频率。
- 通过给出起始和终止时间项来指定测量期间。

性能管理的目的就是确保网络不会出现过度拥挤的情况，保障网络的可用性，为用户提供更好的网络通信服务，它主要采用实时监控网络设备和相应的所有连接，监视设备和线路的使用率和出错率及相应的阈值，并进行阈值报警；实行定期的历史数据分析，及时提示管理者和决策者作出设备或线路的升级计划，保证设备和线路的容量不会由于过度使用而出现网络性能急剧下降的情况。

1.10 服务质量技术

1.10.1 基本概念与相关技术

1.10.1.1 QoS 概述

在通信和计算机网络中，服务质量简称 QoS。QoS 的提出始于 ATM 交换机。 QoS 有广义和狭义之分：狭义 QoS 指技术指标（传输时延、抖动、丢失率、带宽要求、吞吐量等）；广义 QoS 指资源调配与利用、层与层之间的协商，从而涉及不同层次的 QoS。

QoS 在 IETF 中定义为“A set of service requirements to be met by the network while

transporting a flow"，即网络在传输数据流时要满足的一系列服务要求，具体可以量化为传输时延、抖动、丢失率、带宽要求、吞吐量等指标。

因特网的 QoS 是指某个主机上的应用向其他主机上的应用发出一系列的数据包流时的平均速率、最大速率、数据包的延迟时间、抖动、数据包的丢失等。移动通信网络的 QoS 是指某个终端的应用向其他终端的应用发出一系列的数据包流时的平均速率、数据包的延迟时间、抖动、数据包的丢失等。

但是这些值并不是只从网络的结构就能确定的，它具有受流入网络中的通信量影响的特性。就好比高速公路的质量，高速公路的质量应该是时速多少千米，但仅靠公路的结构值是不能预测公路的质量的，它不仅与汽车的流量有密切关系，还与天气状况有关，如大雪封路等。

因特网和移动通信网同样如此。例如，如果不对流入的通信量加以制约，就不可能预测和控制网络内的延迟。不仅由于自己的通信量，还会由于别人的数据量而发生线路速率、误码率和延迟等的改变。

与 QoS 相似的概念是服务等级（CoS）。当网络根据流的质量分为不同等级时，其等级就称为 CoS。

IETF 提出了两种关于因特网的国际服务标准化方法：IntServ 和 DiffServ，即通常说的综合服务和区分服务。

ITU 关于 QoS 问题的研究开展得比较早，最早的相关建议出现在 20 世纪 60 年代，当时的 QoS 主要是指传统电话业务的性能，但是随着 IP 技术在电信领域的应用，QoS 概念的内涵得以扩展。关于 IP QoS 的问题，ITU 发布了一系列的推荐标准（建议），集中在 ITU-T E 800-E 899 系列（电信服务质量：概念、模型、目标与规划）中。这里 IP QoS 的行为主体是指用户、电信业务提供商（SP）、电信网络提供商（NP）。用户与电信业务提供商之间、电信业务提供商与电信网络提供商之间签订 SLA，并按照 SLA 中规定的服务功能和性能指标来确定服务的质量。与 IETF 关于 IP QoS 的定义相比，ITU-T 的 IP QoS 不单指网络层 QoS，还包括应用层 QoS，它从网络运营的角度来定义 IP QoS，认为 IP QoS 存在于各个网络运营实体之间。

由于欧洲电信标准协会（European Telecommunication Standards Institute，ETSI）和 ITU 均属于电信领域的研究机构，并且两个组织的研究人员在 IP QoS 研究领域有重叠，因此 ETSI 对 IP QoS 概念的理解基本上和 ITU 对 IP QoS 的理解相同，均是从网络运营的角度，基于各个网络运营实体来定义的。这一点可以从 ETSI 文档 ETR 003 （服务质量和网络性能的通用概念）中看出。

ISO 的 OSI 网络七层协议栈模型一直是计算机网络协议和电信网络协议设计、分析、实现的重要参考，在 ITU-T X.200（ISO/IEC7498-1）中定义了七层协议栈模型，在这个模型中给出了一些关键的定义（如服务），但是没有给出十分明确的和七层协议栈对应的服务质量的概念。在 ISO/IEC JTC1-SC21 服务质量框架（quality of service framework）中

对这个方面的内容进行了补充，给出了完整的QoS模型和相对完善的QoS定义。ISO认为各个网络层次之间、对等层次之间都存在服务和被服务关系，因此就存在服务质量的概念。因此，QoS不只局限于网络层和应用层，它存在于网络的各个协议层次之间，只要有服务的地方就势必有服务质量的概念。ISO对QoS的定义可以看做IETF，ITU，ETSI关于QoS定义的内涵的超集。

1.10.1.2 QoS分类

目前涉及QoS控制和管理的标准有以下一些：

- 在应用层，ISO/OSI提出了基于ODP（Open Distributed Processing）分布式环境的QoS控制。
- 在网络层，ATM论坛提出了QoS控制的策略和实现。
- IETF RFC2115，RFC2117中的IS（Integrated Service）和DS（Differentiated Service）体系结构，用于解决Internet的QoS控制和管理。
- 在数据链路层，以太网络中提出了802.1p、802.1q以及SBM（Subnet Bandwidth Management）等标准。

通过服务质量控制和管理技术使得分布式系统可以支持多媒体和实时数据的服务，但是不同组织、不同企业所使用的服务质量参数不同，导致各层次上的参数的语法、语义和语用不一致，这使已提出的种种QoS技术难以协同地为建立复杂的分布式系统而服务。

例如，某个异质的分布式系统，由于上述组织中所用的QoS参数不同，使得系统中高层应用程序与下层不同层次中单元的QoS参数含义、表示和度量不同。在资源层次中，QoS参数取决于所使用的资源类型及它们的控制参数，比如在ATM中QoS参数以cell为单位，所表示的是cell的速率、cell的延迟、cell的抖动和cell的丢失率等，而在IETF的IS中以packet为单位，所表示的是packet的速率、packet的延迟、packet的抖动和packet的丢失率等。具体的分布式多媒体应用程序需要在分布式系统上运行，它要求下层（如操作系统层、网络层等）的资源按照应用层所指定的QoS参数（比如ISO/OSI的应用层的服务质量参数标准）的范围进行服务操作。分布式系统的下层资源需要知道上层应用QoS参数的语法和语义，并能在自己的资源上把上层的QoS参数映射为自己所使用的QoS参数类别（例如，IP网络的通信资源所使用的是packet延迟和packet抖动等QoS参数，而具体的分布式视频程序所使用的是帧延迟和帧抖动等QoS参数）。如果存在n个网络层标准和1个应用层标准，那么QoS参数的转换存在$(n+1)!$种可能性，要建立这样的分布式系统是很复杂而且低效的。

为此，要建立一个支持QoS机制的分布式系统，必须建立统一的QoS框架（QoS framework），这一框架包括QoS体系结构（QoS architecture）和QoS规范分类学（QoS specification taxonomy）。其中QoS体系结构完成把与QoS有关的复杂的资源对象结合

起来，以此建立有效的分布式系统；而 QoS 规范分类学是在研究 QoS 参数和它们之间的相互关系的基础上，建立统一的 QoS 参数规范，详细地定义 QoS 参数的含义、表示、度量单位和相互关系，最终使得分布着的各个系统资源组件之间，在 QoS 层面得到统一的转换——QoS 映射（QoS mapping）。这样构筑的基于 QoS 上的框架将为新一代分布式多媒体和实时系统的实现建设打下坚实的基础。

由于以上原因，人们逐渐认识了 QoS 分类学技术的重要性，对各种 QoS 参数进行统一分类，使得 QoS 的映射得以简化和易于实现。

1.10.1.3　QoS 指标参数及管理测量

1．QoS 的主要指标参数

当前网络的服务质量主要有以下一些衡量指标。

1）可用性

可用性是指用户能够使用 IP 业务可用性功能的时间间隔占 IP 业务全部时间间隔的百分比。在连续 5min 内，如果一个 IP 网络所提供业务的丢包率小于或等于 75%，则认为该时间段是可用的，否则是不可用的。可用性主要用于衡量网络设备、链路正常提供业务的能力，确定该网络设备、链路是否能够支持连续可用的数据包传送业务。

2）吞吐量

吞吐量是指网络中 IP 包的传输速率，可表示为平均速率或峰值速率。网络的吞吐量是衡量网络能够成为一个 IP 流转发报的能力，主要取决于链路速率、节点设备的端口速率，以及网络的业务量状况。

3）延迟

延迟是指 IP 包从网络入口点到达出口点所需要的传输时间间隔。造成网络延迟的主要因素如下。

- 传播延迟：是指信号在物理媒介上传输所需要的固有时延，如在光纤上的延迟大约为 5ms 每 1000km。
- 链路速度延迟：数据传送的速度取决于链路的比特率（速率）。当链路速度低于数据发送速度时（如一个 100Mbps 的以太网仅接了一条 2Mbps 的出口链路），便会产生链路速度时延。
- 交换和路由延迟：网络节点转发数据包的时间。对于路由器，这个时间用于分析数据包头，查询存储的状态信息，并检查路由表，最终将数据包转发到输出端口。
- 排队延迟：由于 IP 网络的统计复用和数据包到达的异步特性，在节点的输入和输出端口必然要依次排队，这样数据包才能发送到相应的链路上。排队延迟取决于队列长度和数据包在端口的统计分布。
- 跳数：数据包结构一个交换节点（路由器）被称为一跳（hop），网络传输时延随着跳数的增长而增加，因此减少数据包传送经过的跳数，是控制时延的主要方法之一。

4）丢包率

丢包率是指IP包在网络节点之间传输时丢失的IP包数与已发送的IP包总数的比值。当网络拥塞、传输损伤、超过生存周期（TTL）时，丢包就可能发生。

5）延迟抖动

延迟抖动是指在一段测量时间间隔内，最大IP包传输时延与最小IP包传输时延的差值。由于IP网络采用的协议是面向无连接的，因此不同的包从网络的入口到出口所经过的路由可能不同，所经过的网络的速率可能不同。网络中的节点设备采用的转发决策或拥塞控制机制不同，队列的流量随时间而不同，不同的IP包的转发有可能不同，因此节点设备对IP包的处理时间不同。当IP包从网络入口传送到网络出口时，便会造成IP包的时延变化，即抖动。

上述服务质量衡量指标与接口带宽、网络设备交换能力等资源直接相关。网络用无限的带宽资源和节点交换能力来保证分组层服务质量，这显然是不可能的。但是有普遍观点认为，即使没有无限的资源，网络也可以通过其他方法保证服务质量。正如传统的电话交换网，其传输电路和交换能力都有限，但是电话业务有固定的业务模型和可以预知的业务流量流向，传统电话网的服务质量是可以得到保障的。

2．QoS 管理

1）QoS 管理模型

目前IP网还没有标准的QoS管理模型，只有两个很好的参考模型。

一个是电信管理论坛TMF提出的TOM（Telecom Operations Map）模型。TOM在电信管理网（TMN）的4层结构基础上，对每个管理层面的功能和操作进行了具体的描述，使其适合IP网络的管理。在这个模型中，IP QoS管理主要在业务管理层实现。TOM还将业务的生命周期分为三个阶段：业务开通、业务保障和业务计费。业务开通将用户的QoS要求传送到网络中，并进行相应的配置；业务保障维护协商好的QoS，是IP QoS管理的主要阶段；业务计费进行公平合理的计费。TOM模型最有可能成为运营商和设备制造商提供QoS业务的参考标准。

另一个模型是IETF提出的基于策略的管理框架。这个框架将网络中的一些操作和管理抽象出来，称为策略（policy）。网络管理者事先定义好一些管理策略，存放到策略信息库中，网络设备根据这些策略自动地进行网络操作。由于策略由网络管理者统一制定，因此采用不同QoS技术的异构网能够实现统一的QoS管理。

2）SLA 管理

服务等级协议（Service Level Agreement，SLA）是用户与网络服务提供商（ISP）签订的关于服务质量的协议。ISP根据SLA来对用户提供某个等级的服务和计费。SLA分为静态和动态两种。静态SLA在一定的时间范围内是不变的，与网络的状况（如拥塞程度、负荷变化）无关；动态SLA根据网络的状态来协商和调整SLA参数，从而提高网络的资源利用率。当前，大部分网络仍采用静态SLA，而动态SLA还处于研究阶段。

SLA中包括一个或多个流量调节协议（Traffic Conditioning Agreement，TCA），SLA

和 TCA 都属于商业上的协议，它们的技术细节分别由服务等级规范（Service Level Specification，SLS）和流量调节规范（Traffic Conditioning Specification，TCS）来表述。目前的研究主要集中在 SLS 和 TCS 的内容定义。SLA 的建模和标准化是当前研究的重要问题。

3）QoS 资源管理

在 QoS 管理过程中，需要对用户的业务进行接纳控制。IntServ 可以通过资源预留来达到这一目标，但是 DiffServ 还不能实现端到端的资源预留和接纳控制。为了解决这个问题，出现了带宽代理（Bandwidth Broker，BB）。

BB 实际上就是一个资源管理器，它收集网络的拓扑和节点及链路状态信息，管理网络资源，并结合策略服务器规定的策略进行接纳控制，DiffServ 域之间通过 BB 进行 SLA 协商，使 DiffServ 能够实现端到端的接纳控制和 QoS 保障。当前，BB 的研究是实现 QoS 管理的又一个重要环节。

3．QoS 的测量

QoS 测量是一个新的研究课题，它的目的是用测量手段取得网络的性能和服务质量指标。显然，网络的 QoS 控制、维护、管理和计费都需要 QoS 测量的支持。QoS 测量有不同的分类方法，按照测量过程中测试设备是否主动发送探测包，可分为主动测量和被动测量两类；按照测试设备所处的位置，又可分为基于路由器的测量、端到端测量，以及路由器协助的测量。QoS 测量的内容很广泛，包括网络拓扑发现、时延、丢包率、带宽测量，网络距离测量，路由器调度策略和瓶颈缓冲器容量测量，以及路由器流量监测。

QoS 测量需要复杂的技术。特别是端到端 QoS 测量，在没有路由器参与，两端设备时钟又不同步的情况下，利用信号处理技术和数学分析方法，可以推测网络拓扑，端到端的单向传输时延、链路时延、链路带宽、路径上的瓶颈带宽及可用带宽，甚至还可以推测网络中路由器的调度策略和缓冲器容量。端到端 QoS 测量具有特别重要的意义，它可以测出网络的整体性能指标，而且不需要对路由器进行改造，也不需要网络运营商公开内部资料（如网络拓扑、设备配置、传输容量等）。

4．SLA、SLS、TCA 和 TCS 的相互关系

当乘火车时，乘客需购买火车票，铁道部门提供运输服务。乘客除了要指定目的地、出发时间以外，还要指定软卧、硬卧或硬坐等座位种类。如果列车已经超载，铁道部门会拒绝乘客搭乘（接入控制），甚至乘客携带物品的种类、大小、重量、个数也有限定（流量调节）。当乘客接受列车服务时，可以指定服务质量，但要接受携带物品的限制。

同样，对于网络服务，使用者可以指定流的 QoS，为了接入其服务，流的特性（速率、最大脉冲长度等）有义务保持在事先约定好的数值以下。也就是说，对于 QoS 服务，使用者购买的数据流的传输负荷与网络经营者提供的 QoS 水平有着不可分割的关系。

使用者在利用网络服务开始之前，需要通知网络所希望的 QoS 服务水平。网络在拥

塞时有可能会拒绝提供服务（接入控制）。在使用网络服务时，每次使用者投入的流量、使用者希望的 QoS 服务水准（这两者一起叫做流规格说明）与经营者可以提供的 QoS 服务相对照，通信经营者与使用者必须制定一个两者都同意的 QoS 服务等级。

使用者和经营者商量好的内容就叫做 QoS 服务等级协议 SLA。SLA 的内容包括服务方式、流量规格、使用费用、用户以及网络经营者双方没有履行合同规定时的惩罚条例等。

在 SLA 中技术的部分被称为服务等级规范 SLS。流量调节协议 TCA 是指数据包分类准则和描述业务流暂时特性的流轮廓（如速率和突发数据包大小）。SLA 中关于流的 QoS 服务等级及其流量说明的部分叫做流量调节规范 TCS，TCS 是 TCA 的技术部分。

SLA、SLS、TCA 和 TCS 的相互关系如图 1-138 所示。其中，SLA 包括 TCA 和 SLS，SLS 包括 TCS，TCA 也包括 TCS。

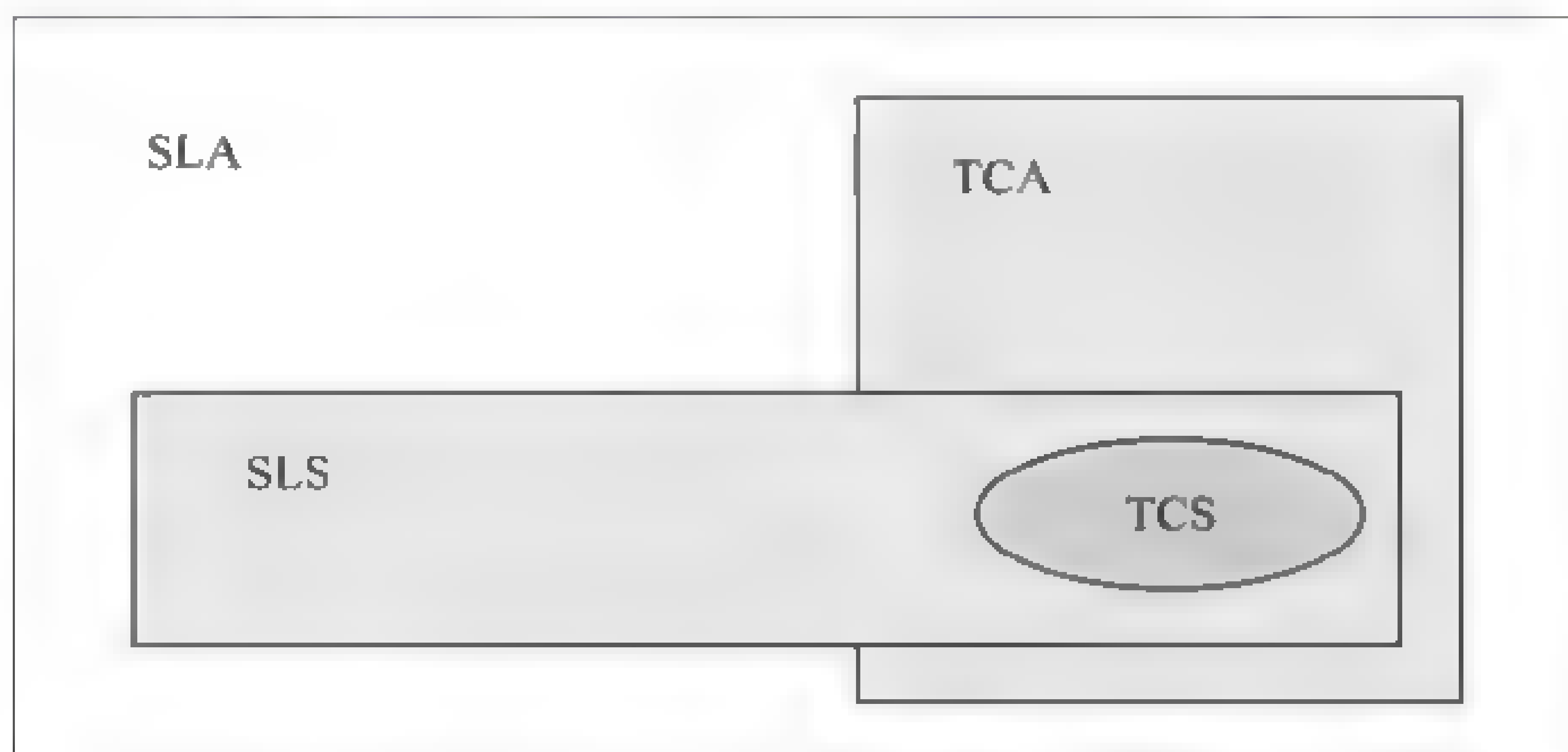


图 1-138　SLA、SLS、TCA 和 TCS 关系

1.10.2　IP 网络 QoS 技术

现有的 Internet 最初是面向非实时的、单种数据类型通信（如文件传输、E-mail）设计的。IP 协议提供一种无连接的网络层，必须辅以其他高层端到端协议（如 TCP）才能更好地实现端到端的可靠传输。由于 Internet 设计时没有关注 QoS 控制和管理技术，所以资源完全共享，资源的访问和使用没有进行有效的控制和管理，不能保证网络按照用户所需的质量要求投递。由于缺少必要的对服务质量的控制和保证，这种传统 IP 传输服务被称为尽力而为型服务（best effort service）。

尽力而为型服务无法给传输提供好的服务质量保证，于是 IETF 借鉴 QoS 技术，加强实现资源的控制和调整机制，使得网络能够支持多种服务，既能保证有服务质量需求者的服务，又能为原有的尽力而为型服务，为此提出了一种体系——综合服务体系（integrated service architecture）。其主要目的是在基于 IP 的网络中提供一定级别的服务质量。在 IntServ 中将通信业务分为两大类：有弹性通信业务（elastic traffic）和无弹性通信业务（non-elastic traffic）。

有弹性的通信业务能够忍受延迟、流速的变化，它是一种自适应的应用。有弹性的

应用程序能够动态地调整其对网络的使用，试图使用最大的带宽。但是，当网络明显拥挤时，它采用退避算法自适应网络的变化。目前 Internet 是适合有弹性的通信业务的。

无弹性的通信业务对延迟、速率、抖动和丢失率都十分敏感。无弹性的应用程序遵循的原则是："要么给我有服务质量的网络，要么什么都不给"。交互式语音、视频和实时任务是无弹性通信业务的典型例子，它要求服务质量在应用允许的范围内。目前 Internet 不适应无弹性通信业务，特别是在网络拥挤时。

1.10.2.1　综合服务（IntServ）体系

1．IntServ 服务质量控制的组件

IntServ 的目的是在基于 IP 的网络中提供服务质量。IntServ 力图解决在网络发生拥塞时如何共享可用的网络容量的难度。IntServ 使用具有以下功能的服务质量控制组件。

- 接纳控制：对于服务质量传输（而不是默认作尽力而为型传输），IntServ 要求对一个新的流要进行预留。如果网络内的路由器共同认定没有足够的资源来保证所请求的服务质量，则这个流就不允许进入网络。
- 路由选择算法：可以基于许多不同的服务质量参数（而不仅仅是最小时延）来决定路由的选择。例如，路由协议为 OSPF 就可以基于 QoS 来选择路由。
- 调度算法：IntServ 的一个重要元素就是有效的排队和调度策略，它考虑不同流的不同需求。
- 丢弃策略：如果有许多数据包在输出端口排队，当数据包使用完缓冲区之际，在管理拥塞和满足 QoS 保证时，数据包的丢弃策略就是服务质量一个重要元素。

IntServ 中专门使用服务质量控制服务（QoS control service）这一术语，它是指网络元素所提供的服务质量控制功能协同工作的集合，其中网络元素包括路由设备和端节点。

2．IntServ QoS 组件在路由器上的实现

在 RFC 1633 规范中指出了 IntServ 整体解决方案。图 1-139 是一个路由器的 IntServ 实现体系结构，包括 6 个组件，在粗的水平线下面是路由器的转发功能，这对每个数据包都要执行，因此必须很好地进行优化。在水平线以上的一些功能是背景功能，用来产生转发功能所使用的一些数据结构。

- 资源预留协议 RSVP（RFC2205）：它是 Internet 上的信令协议。通过 RSVP，用户可以给每个业务流或连接申请资源预留，要预留的资源可能包括缓冲区及带宽的大小。这种预留需要对路径上的每一跳都要进行，这样才能提供端到端的 QoS 保证。RSVP 是单向的预留，适用于点到点及一点到多点的通信环境。
- 接纳控制：当一个新的流请求时，预留协议就调用接纳控制模块。这个功能模块要判断对这个流所请求的 QoS 是否有足够的资源可提供，这个判断是根据当前已对其他预留的承诺及网络的当前状况而做出的。

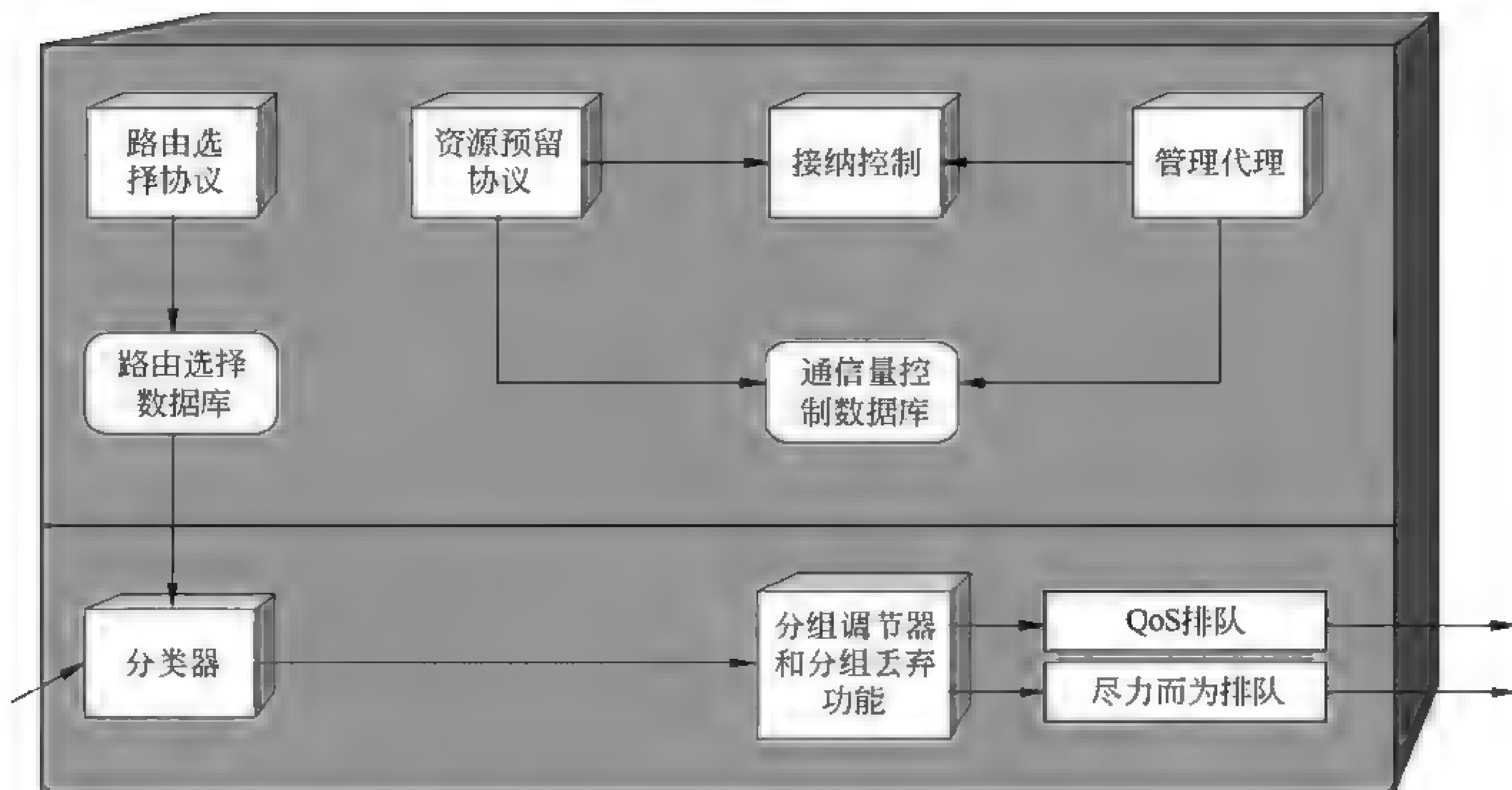


图 1-139　路由器中实现的 IntServ 体系结构

- 管理代理：网络的管理代理，能监督接纳控制模块，并且设置接纳控制的策略；同时它能够修改通信量控制数据库，以影响队列调度和分组丢弃。
- 路由选择协议和路由选择数据库：通过对 IP 数据包分类，路由算法可以根据 IP 数据包的类型、最小代价及其他服务质量参数进行路由选择，同时此路由还维护一个路由数据库，它对每个目的地址和每个流都给出应到达的下一跳。
- 分类器：根据预置的一些规则，它对进入路由器的每一个分组进行分类。这可能需要查看 IP 分组里的某些域：IP 源地址、IP 目的地址、上层协议类型、源端口号、目的端口号；分组经过分类以后被放到不同的队列中等待接收服务。 这个功能决定此分组的下一跳地址。
- 分组调度器和分组丢弃功能：分组调度器主要是基于一定的调度算法对分类后的分组队列进行调度服务。它决定排队的分组发送顺序，当网络发生拥塞时应丢弃哪些分组。做出决定要基于分组的类，通信量控制中的内容以及输出端口过去和现在的活动情况。分组调度器的部分任务是监管，这种功能判断是否在一个给定的流中分组的通信量已超过了所请求的容量。如果是这样，则应决定如何处理这些超量的分组。

3．IntServ 的服务分类

在 IntServ 中定义了三种服务类型：QoS 保证服务型（Guaranteed Service，GS）、受控负载服务型（Control Load Service，CLS）和尽力而为服务型（Best Effort Service，BES）。

- 保证服务型（RFC 2212）：这种服务等级提供明确的参数级别，有排队延迟上界、

绝对不会因为排队而丢失数据包。GS 提供设定延时的确定带宽，不会因为网络拥塞而丢失数据包。虽然它类似 ATM 的 CBR 业务，但是它们是有区别的。GS 即使通过调整整体服务速率、排队延迟也仅在一定程度上受控，同时仍然无法使整体的延迟抖动最小化；GS 保证数据不丢失，这一点不同于 ATM；GS 适合于实时任务，它们要求数据报在有保证的时间内投递到目的地，不会因为队列溢出而丢失数据包。

- 受控负载服务型（RFC 2211）：这种服务等级在不拥挤且负载较轻的网络中提供近于尽力而为型服务。与 GS 不同，它不能对排队延迟设置上界，也不能保证不会因为排队而丢弃数据包。这种服务意味着对大部分业务量都能够成功地传递，而且还可以用于能适应网络状况波动的实时应用程序。CLS 不会对有保证的服务或尽力而为的服务产生影响。
- 尽力而为服务型：这种服务等级不提供任何保证。这就是目前 Internet 所提供的服务。当网络比较宽松时，用户能获得较好的服务；然而，当网络拥挤时，用户所获得的服务也随之下降。

4．IntServ 的服务资源预留协议（RSVP）

IntServ 中定义 RSVP 为其 QoS 信令。通过 RSVP，用户可以给每个业务流申请资源预留，要预留的资源可以包括缓冲区及带宽的大小。这种预留需要在路径上的每一跳都进行，这样才能提供端到端的 QoS 保证。

利用资源预留可以使路由器能够提前决定是否有能力满足传输该协议，为每个流预先申请要求的网络资源，在 IP 分组从源端到接收端之间所要经过的每一个路由器上为每个流申请所需要的带宽、缓冲区等资源，路由器必须为每个流保持所需要的“软状态”。所谓软状态是进行资源预留时周期性控制的临时状态，它包括有关该流的源、目的地址、路由信息、需占用该路由器的资源信息等，它不需要明确的删除请求，而由周期性的 RSVP 消息刷新。IntServ 利用 RSVP 协议提供端到端的信令控制，以使无连接的 Internet 网对于某些业务（实时业务）变成有连接的网络。RSVP 提供不同的预留模式，以允许应用选择不同的资源预留的合并方式。

在 RSVP 协议的机制中，设计了两个基本报文类型：Resv（预留）和 Path（路径）。Resv 报文是多播组的接收者发出的，沿着分发树向上游传播，在传播路径的节点上会根据需要进行合并和组装。这些报文在分发树上的路由器中创建了软状态，而分发树就反映了为本次会话（对应于一个多播地址）所预留的资源。最后，合并了的 Resv 报文到达发送主机，使得主机能够为第一跳的传输设置恰当的流量控制参数。

由于 Resv 报文必须向上游传播，经过所有中间路由器，最终到达所有的发送主机。然而路由选择协议缺少反向路由信息，因此 RSVP 引入了 Path 报文。作为发送者参加多播组的所有主机都要发出 Path 报文，经由分发树传输到所有的多播终点。Path 和 Resv 报文的转发如图 1-140 所示。

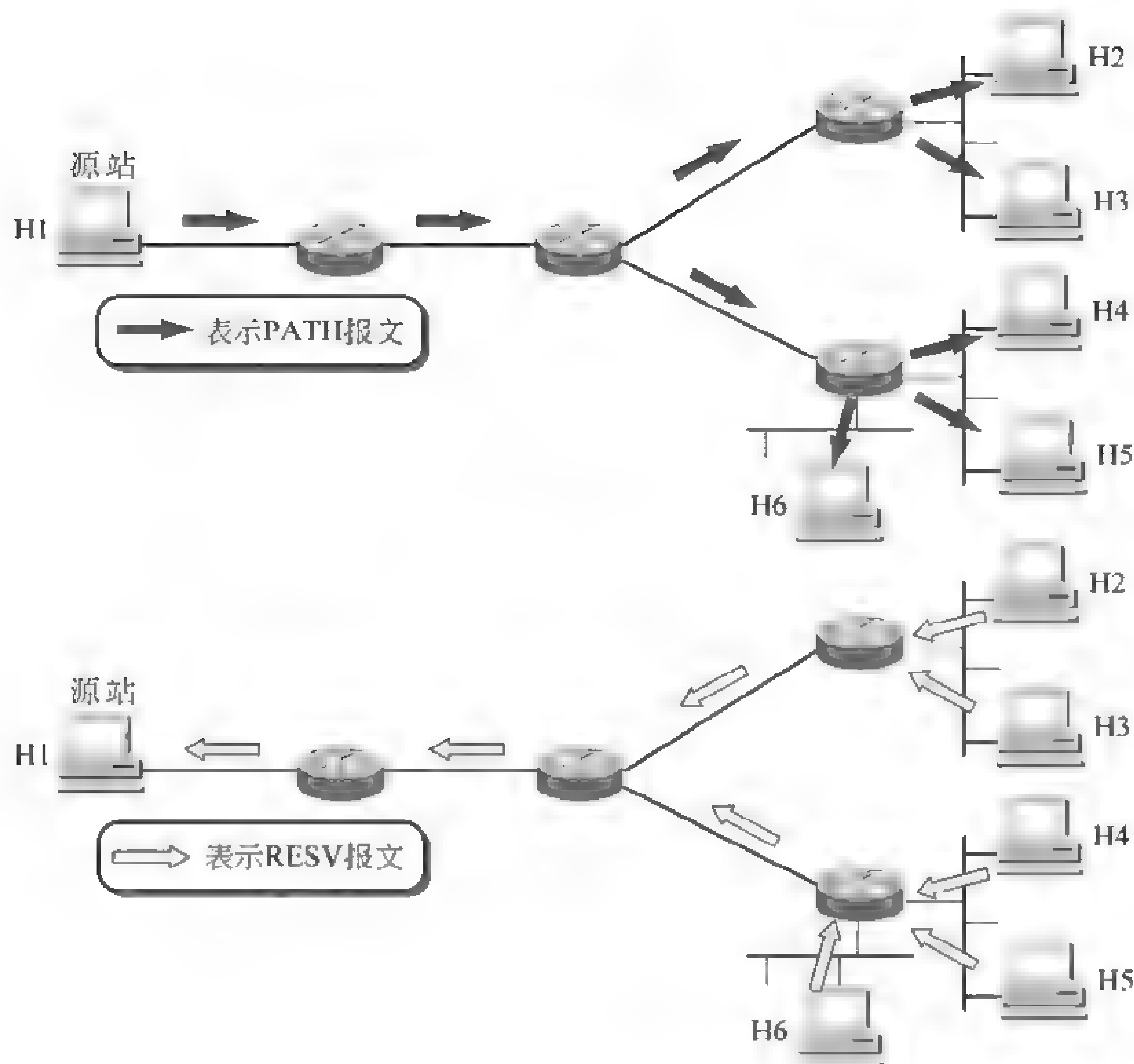


图 1-140　PATH 和 RESV 报文的工作原理

RSVP 协议资源预留过程如下：

① 发送数据的源端确定发送数据流所需的带宽、延迟和延迟抖动等指标，并将其包含在 PATH 分组中发给接收端。

② 在网络中的某一路由器接收到 PATH 分组时，它将 PATH 分组中的路径状态信息存储起来，该路径状态信息描述了 PATH 分组的上一级源地址（即发来该分组的上一跳路由器地址）。

③ 当接收端收到 PATH 分组之后，它沿着与 PATH 分组中获取的源路径相反的方向发送一个 RESV 分组。该 RESV 分组包含为数据流进行资源预留所需要描述的流量和性能期望等 QoS 信息。

④ 当某一路由器接收到一个 RESV 分组时，它通过接纳控制来决定是否有足够的资源满足 QoS 请求。如果有，就进行带宽和缓冲区空间的预留，并且存储一些与数据流相关的特定信息，然后将 RESV 分组转发给下一个路由器；如果路由器必须拒绝该请求，则它返回给接收端一个错误信息。

- 如果源端接收到 RESV 分组，则表明数据流的资源预留已经成功，可以开始向接收端发送数据。
- 当数据流发送完毕，路由器可以释放先前设置的预留资源。

5. IntServ 体系结构的进一步探索

IntServ 能为用户提供 QoS 保证，但在具体的实现中还存在扩展性较差的缺点，因为其工作方式是基于每个流的情况，这就需要在路由器中维护保存大量的与分组队列数成正比的状态信息。此外，RSVP 的有效实施必须依赖于分组所经过的路径上的每个路由器。在骨干网上，业务流的数目可能会很大，同时它还要求路由器的转发速率很高，这使得 IntServ 难以在骨干网上得到实施。为了解决 IntServ 的一些缺点，IETF 在 RFC 2475 中提出了区分服务体系。区分服务体系旨在定义一种既能实施 IP QoS 又能更容易扩展的方式，以解决 IntServ 所存在的缺点。

虽然 IntServ 体系结构中存在以上缺点，但是它相对于 DiffServ 而言，属于细粒度 QoS 控制，即可以为高层用户提供较为准确的带宽、延迟、延迟抖动和丢失率控制，而 DiffServ 属于粗粒度 QoS 控制，无法为高层用户提供精确的 QoS 控制，所以 IntServ 仍有其存在的生命力。目前，比较一致的看法是在企业网的边缘实施 IntServ，而在企业的骨干网络中使用 DiffServ。

以 IP 技术为基础的 Internet 正朝着宽带化、服务综合化方向发展，而作为合格的宽带综合服务数字网络必须要能满足不同业务的服务质量要求。为此，未来值得探索的方向如下。

1）队列管理机制（queue management mechanism）

在网络发生拥塞时，路由器必须丢弃一些分组，这个问题的解决首先必须实施有效的队列管理机制（或缓冲区管理策略）。

目前，已经出现的队列管理机制有 PPD（Partial Packet Discard）、EPD（Early Packet Discard）、RED（Random Early Discard）、FRED（Flow RED）、RIO（RED with In and Out）等算法。比较起来，RED 算法具有较低的排队时延、较高的分组通过率和较好的公平性，其主要思想是：路由器计算平均排队长度，当平均排队长度超过某一门限时，路由器按照一丢弃概率丢弃到达的分组，而这个丢弃概率是与平均排队长度成正比的函数。RED 算法允许短时的分组突发，因而可以避免因为网络负荷变化造成的分组丢弃；RED 能避免多个 TCP 连接同时的超时重传，从而保持高的带宽利用率；此外，RED 算法还能较好地支持突发业务，且确定哪些连接使用了更多的带宽，并可以采取措施予以惩罚。FRED 和 RIO 都是对 RED 的改进或变种，FRED 对每一个业务流（或连接）都实施单独的一个 RED 算法，这样能保证更好的公平性；RIO 在 RED 基础上又增加了一个门限值。

2）队列调度机制（queuing scheduling mechanism）

不论在 IntServ 还是在 DiffServ 里，都涉及队列调度问题。简言之，队列调度的功能

就是路由器如何从一个或多个队列中选择下一个将转发的分组，这与队列管理机制有着本质的区别。一个有效的队列调度算法应达到的性能指标主要有公平性、时延特性、对恶意业务流的隔离能力、链路带宽的利用率、复杂性等。前 4 个指标与 QoS 密切相关。目前主要有 Weighted RR、Deficit RR、加权公平排队（WFQ）、自时钟公平排队（SCFQ）、VC（Virtual Clock）等算法。

在队列调度算法研究中，如何提供较好的公平性、时延特性，同时算法复杂度较低且易于实现的特性成为人们关心的焦点。

3）基于 QoS 约束的路由（constrained-based routing）

基于约束的路由（CBR）源自 QoS Routing，只是对 QoS 的限制参数进行了一定的扩充。基于约束的路由的有效实现需要各个路由器之间的相互配合，比如相互通知各自所知道的网络的一些状态信息（如链路的剩余带宽）。其难点在于：如何在状态信息的精确发布和发布频率之间取得一个折中。因为链路的剩余带宽在不断的变化，基于约束的路由既要避免状态信息发布的滞后性，又要避免不停地频繁发布状态信息。基于 QoS 约束的路由的有效实现还有待进一步研究。

1.10.2.2 区分服务体系

1. 区分服务（DiffServ）

综合服务（IntServ）体系和 RSVP 的设计目标是在因特网和专用互联网上支持 QoS 功能。虽然 IntServ，尤其是 RSVP 对于完成这样的目标都是有用的，但这个功能的实施却很困难。另外，它们不容易进行规模扩展以支持较大的通信量，因为用来进行综合 QoS 支持协调的控制信令的数量很大，而且在路由器上维护状态信息。

随着因特网负担的加重以及应用种类的增多，对于不同的通信流提供不同水平的 QoS 是一个紧迫的需求。区分服务体系结构（RFC 2475）的设计目标是提供一种简单的、容易实现并且是低成本的工具来支持一系列的网络服务，这些服务在性能的基础上有所区分。

DiffServ 其实现途径如下：

- 简化网络内部节点的服务机制。在内部节点只进行简单的调度转发，而流状态信息的保存与流监控机制的实现等只在边界节点进行时，内部节点是与状态无关的。
- 简化网络内部节点的服务对象。采用聚集传输控制，服务对象是流聚集（stream aggregate）而非单流，单流信息只在网络边界处保存和处理。

具体而言，边界节点根据用户对流的轮廓描述和资源预留信息将进入网络的单流分类、聚合为不同的流聚集，这种聚集信息存储在每个 IP 包头的 DS（Differentiated Service）标识域中，称为 DiffServ 码点（Differentiated Service Code Point，DSCP）。内部节点在调度转发 IP 包时根据包头的 DSCP 选择提供特定质量的调度转发服务，其特性称为逐跳行为（Per-Hop-Behavior，PHB）。网络边界对单流作分类聚合和网络内部对聚集流提供

特定质量的调度转发服务，这两个过程是依靠 IP 包头内的 DSCP 联系起来的。

除了实现简单外，区分服务体系还具有以下特点：

- 层次化结构。分为 DS 域 （DS domain）与 DS 区（DS region）两级。在 DS 域内，服务提供策略以及 PHB 的语义和实现要一致，但 DS 区内的各 DS 域可以支持不同的 PHB，有不同的服务提供策略，它们之间通过服务等级协议 SLA 与流量调节协议 TCA 协调提供跨域服务。这种结构适应了 Internet 中由各 ISP 提供接入服务的商业模式。
- 总体集中控制策略（与 IntServ 分布式控制相对照）。网络资源的分配由总体服务提供策略决定，包括在边界如何分类聚合流，在内部如何调度转发流聚集。
- 利用面向对象的模块化思想与封装思想，增强了灵活性与通用性。各逻辑模块相对独立，并有多种组合。少量模块可组合实现多种服务，并在发展过程中保持模块的可重用性。例如，服务类型与边界调节器（conditioner）和内部 PHB 相对独立，使得较少种类的边界调节器和内部 PHB 可进行各种不同的组合而实现多种服务类型。再如，PHB 与其具体实现机制相分离，使 PHB 可以在发展中保持相对的稳定，这给商家留下了施展的天地。
- 不影响路由。与一些以虚电路方式实现 QoS 的方案（ATM，MPLS）以及服务类型标记方案不同，区分服务节点处提供服务的手段仅限于队列调度与缓冲管理，不涉及路由选择机制。

2．DiffServ 体系结构

区分服务体系结构的框架如图 1-141 所示。

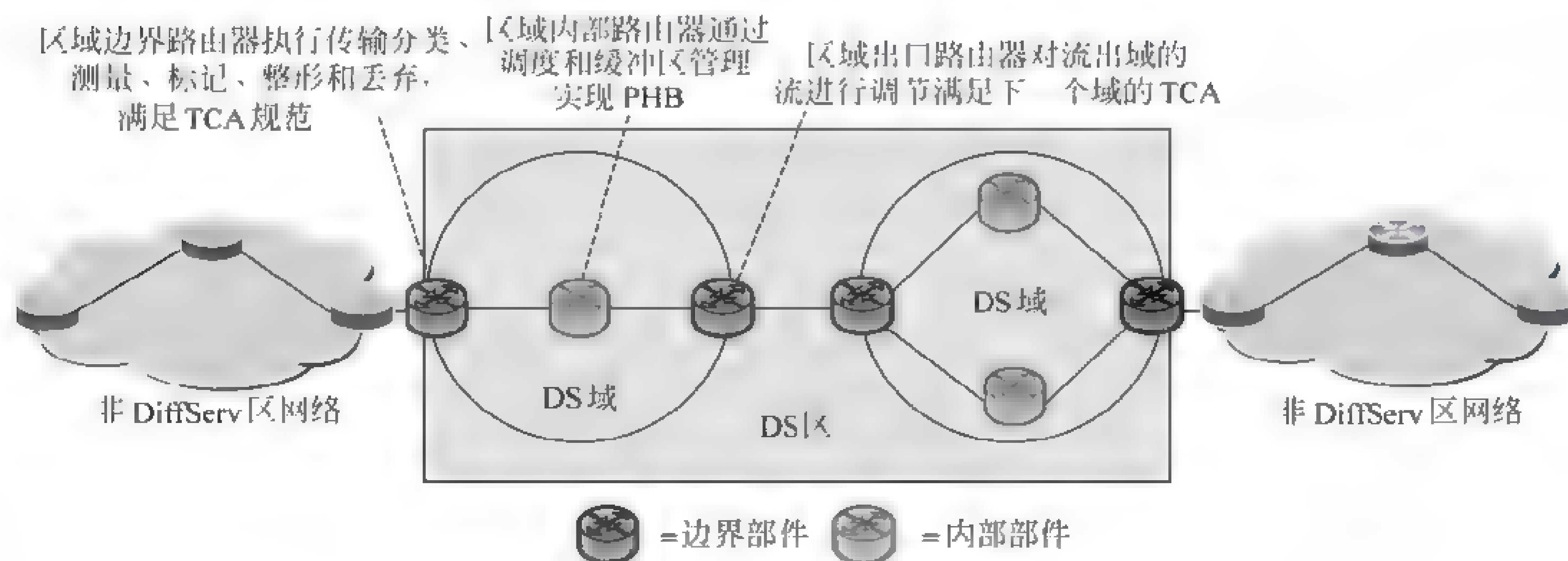


图 1-141　区分服务体系结构框图

1）DS 域与 DS 区

一个 DS 域由一组连续的路由器组成，即从该域中的任何路由器到该域的任何其他

一个路由器都有一条不包括域外路由器的路径。在一个域内，对 DS 码点的解释是相同的，因此可以提供相同的和一致的服务并实现一致的 PHB 组。DS 域有明确定义的边界，边界由边界节点（boundary mode）构成。边界节点连通 DS 域和非 DS 域（或其他 DS 域），其主要功能是：实现传输的分类（classify）和调节（condition）机制（逻辑上表现为分类器与调节器）；保存流（单流或聚集流）的状态信息；根据预定的流规格对进入（或离开）域的流进行调节，包括测量（metering）、标记（marking）、整形（shaping）、丢弃（dropping）几个动作，使输入流（或输出流）符合预先规定的 TCA，并在包头标记 DSCP 值，进行分类且归入行为聚集（behavior aggregate）。需要注意的是，边界节点上也要实现 PHB。

针对特定的流，边界节点又分为入口节点和出口节点。入口节点必须对入域流进行调节，从而确保其符合本域的 TCA 规范；出口节点可能对出域流进行调节，从而保证其符合下游 DS 域所规定的 TCA。

在内部节点上实现一组或若干组 PHB。处理 IP 包时根据包头的 DSCP 值选择特定的调度转发行为。这一过程是多对一的映射（函数），即每个 DSCP 值只能对应一个 PHB，多个 DSCP 可能对应同一 PHB。这种映射关系在一个 DS 域内应保持一致。内部节点的处理对象是流聚集，数量有限，因而处理的时间与空间复杂度低。一般 DS 域由毗邻的属于同一网络管理机构的网络构成，如某个 ISP 的网络或者内部网。

连续的 DS 域构成 DS 区，区内支持跨越若干域的区分服务。区内的各域可能支持不同的 PHB 组，并且各个域的 DSCP 到 PHB 的映射函数也可能不同；如果有不同 DS 域，则域之间必须有 SLA 与 TCA 定义着域间的调节规则，协调彼此的服务语义。域间边界节点分别对出域流与入域流进行调节，以保证其符合 SLA 与 TCA 的规定。

2）区分服务标记域与区分服务码点 DSCP

IP 包头的区分服务标记域（DS field）是 DS 域的边界节点与内部节点间传递流聚集信息的媒介，是连接边界的传输分类和调节机制与内部 PHB 的桥梁。DS 标记域定义为原 IPv4 包头的 TOS 字节或 IPv6 包头的流类型字节（traffic class octet）的前 6 位，如图 1-142 所示。CU 未在区分服务体系中定义。DSCP 是区分服务标记域中的具体值，用来标识数据包所属的流聚集，供数据包经过 DS 节点时选择特定的 PHB。DS 节点上 DSCP 到 PHB 的映射在具体实现中必须是可配置的。定义 PHB 时，应同时指定对应 DSCP 的推荐值。

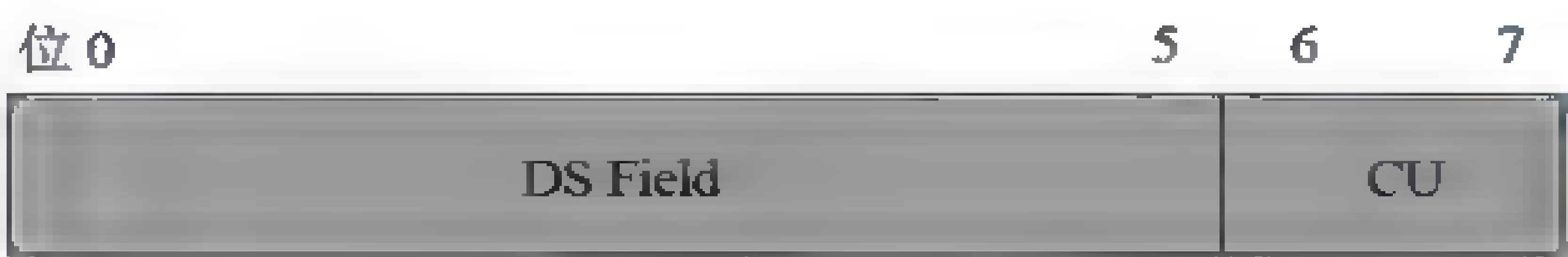


图 1-142 IP 包头的区分服务标记域

3）边界节点的传输分类与调节机制

边界节点要根据 TCA 对入域（或出域）流进行分类和调节，以保证输入（或输出）流满足 TCA 中规定的规范，并将其归入某个行为聚集、标记相应的 DSCP 值。逻辑上分为分类器（classifier）与调节器（conditioner）两个模块，如图 1-143 所示，其各部分含义如下。

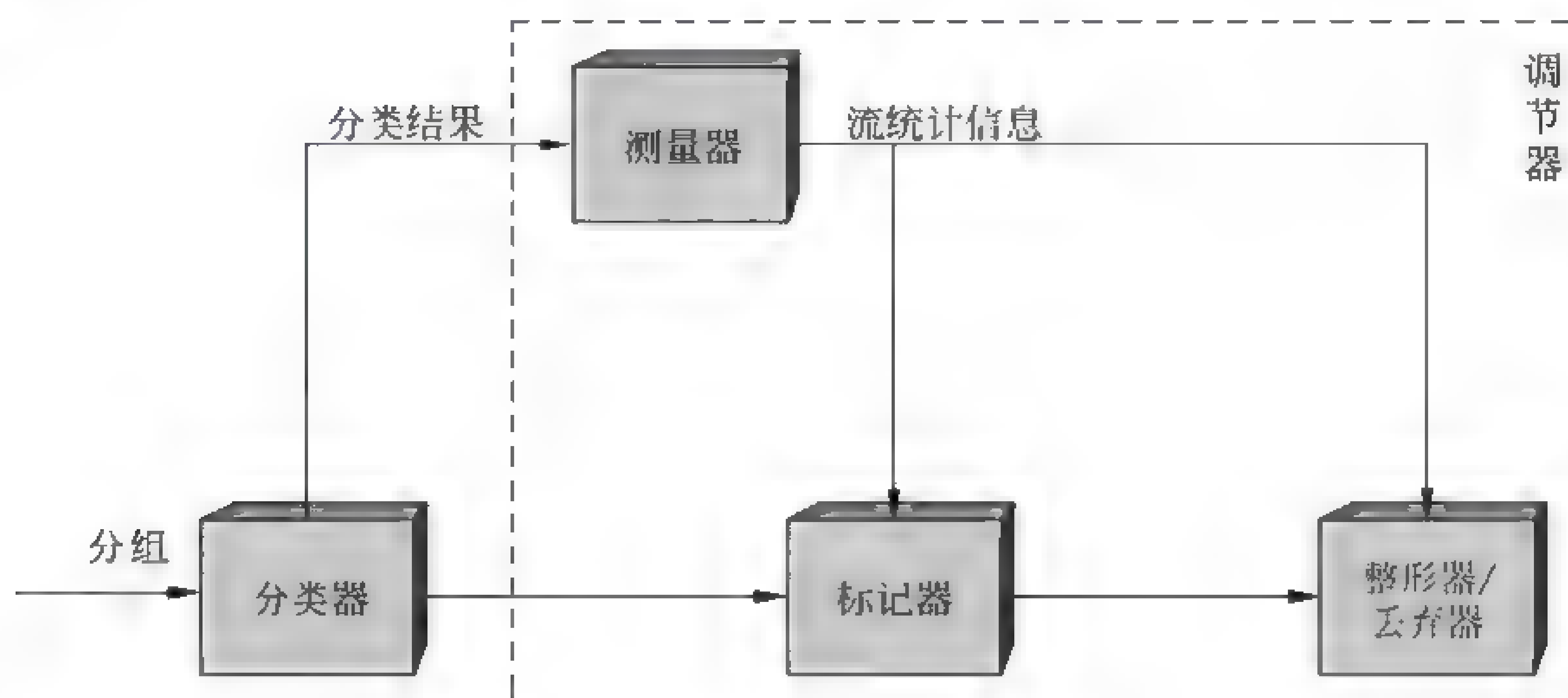


图 1-143　边界节点分类和调节逻辑框图

- 分类器：遵照 TCA 中的特定规则，根据包头的某些域（如 DSCP 值）将包划归某一类别，然后交由相应的调节器进一步处理。调节器在逻辑上分为测量器、标记器、整形器和丢包器。
- 测量器：测量提交的通信量以验证它是否符合 TCA 的流规范。测量器要判断给定的分组流类是否处在或者超出了为该类保证的服务。同时将统计信息传给标记器、整形器和丢包器。
- 标记器：在包头的 DS 标记域中标记适当的 DSCP，即将分组划入某个行为聚集。标记器可以将经过分类器分类后交给它处理的所有分组标记为同一 DSCP 值，也可以根据测量器的统计信息将其标为同一 PHB 组内不同 PHB 所对应的 DSCP 值（例如，确保服务）。
- 整形器：监管通信量，其方式是按照需要延迟分组以便给定类别中的分组流不超过该类 TCA 的流规范要指明的通信量速率。
- 丢弃器：通过丢弃手段强制入流（或出流）符合 TCA 的流规范。

调节器的实现技术比较成熟，只要用令牌桶（token bucket）、漏斗桶（leaky bucket）等算法适当组合即可。通用调节器可以通过合理设置参数来实现优质服务（Premium Service，PS）、确保服务（Assured Service，AS）等服务需要的调节器。当然，某种服务所需要的特定调节器也可以单独实现，其优点在于简单有效。如 PS 用令牌桶做整形、丢弃，AS 也可以用层次化的测量器与标记器实现。总之，调节器的实现形式是多种多

样的。

4）逐跳行为（PHB）

作为DS标准化工作的一部分，需要定义特定类型的PHB与特定的区分服务相联系，目前已标准化的PHB有加速转发型（Expedited Forwarding，EF）、确保转发型（Assured Forwarding，AF）、尽力而为型（Best Effort，BE）以及兼容IP优先级的类选择型（Class Selector，CS）4种。此外，准尽力而为型（Lower than Best Effort，LBE）、允许丢失的加速转发型（Expedited Forwarding with Dropping，EFD）以及协同PHB组（Interoperability PHB group，PHB-I）也正在讨论发展中。

3．区分服务的服务类型

自区分服务概念出现以来，优质服务（PS）与确保服务（AS）是讨论最为集中的两种典型服务。最初分别由Van Jacobson和David D.Clark提出，正是对这两种服务的深入讨论导致了EF与AF的产生。

1）优质服务

优质服务为用户提供低延迟、低抖动、低丢失率、保证带宽的端到端（网络边界到边界）的传输服务，是目前所定义的服务级别最高的区分服务种类。“三低一保证”的服务承诺使得用户可以享受类似专线的服务质量，因而优质服务也称为“虚拟专线”服务。由于PS的服务承诺针对用户流的最高速率，资源预留量也根据最高速率计算，因而为PS所付出的代价也最昂贵。但PS并非要取代传统的BE服务，而是与之共存以提高网络资源的利用率，因为PS没有用尽的带宽可以分配给其他的流（如BE）使用。实际上，PS流只会占据很小一部分资源。最终结果是，ISP的收入提高了，资源也不会闲置。

由于延迟、抖动、丢失主要由于分组在传送路途中排队所致，因而“三低一保证”实际上意味着传输流在传送路途中几乎不排队。而在路由器处出现排队的原因是在某些较短时间段内分组的入速率超过出速率（即请求速率超过处理速率）。因此，最终结论是：任何时刻，在PS流传送道路上的任何节点处都要保证：“PS分组的入速率小于出速率”，或更进一步，“总体上的最大入速率要小于最小出速率”。因此，提供这种服务要确保两点：

- 在传送节点处保证PS流有“良好定义”的最小出速率。“良好定义”意为最小出速率不依赖于节点状态的动态变化，具体而言，不依赖于此节点处其他流的强度。
- 调节PS流（通过整形或丢弃），以保证它在任何节点处的入速率都小于此处的最小出速率。

EF PHB保证前者，后者由边界调节机制实现。

EF PHB定义为一种逐跳行为，它保证任何时候接受此服务的流的离开速率大于或等于设定速率，而且这种保证不受其他传输流的影响。因而与其他PHB共存时，EF总是优先级最高的。

在网络边界处，必须对PS流进行调节，以保证其符合约定的流规格，不超过额定最小出速率。这可以用令牌桶做整形与丢弃来实现。对EF模拟测试的结果，表明EF PHB

与边界调节器的适当实现可以得到预期的“虚拟专线”服务。

2）确保服务

与 PS 的相对成熟、稳定相比较，AS 目前仍处于不断改进和发展的阶段。AS 的初衷是在网络拥塞的情况下仍能保证用户拥有一定量的预约带宽，使用户摆脱在尽力而为型时无法把握自己所占带宽量的无奈窘况。所以，其着眼点是带宽与丢失率，而不涉及延迟、抖动等。服务原则是：无论是否拥塞，都保证用户占有预约的最低限量的带宽；当网络负载较轻而有空闲资源时，用户也可以使用更多的带宽。用户最终得到的带宽分为两部分：

- 预定最小保证值。
- 与其他 AS 流或 BE 流竞争剩余资源获得的额外带宽。与 PS 对带宽的严格承诺不同，AS 着眼于统计性保证，这样可以提高资源利用率并降低价格，但也弱化了服务质量保证。

对 AS 的大量模拟测试表明，AS 的实际服务质量与诸多因素相关，较难达到量化标准，而更多的是一种较优服务。

AS 实现的基本思路如下：

- 分组进入网络时在边界节点给包做标记，预约带宽以内的流量标为IN（in profile），超出预约带宽的流量标为 OUT（out of profile）。
- 拥塞时包头标记决定着分组的丢弃概率，OUT 的丢弃概率大于 IN，从而一定程度上保护 IN 流；中间节点调度转发时保证源头相同的流不乱序，不管其中分组是 IN 还是 OUT。

这种方法的优点是简单。内部节点不需要做什么工作。在边界节点上基于 TCA 中规定的规范对通信量进行标记可以对不同的类提供不同级的服务。

在 DiffServ 体系中，定义了 4 个 AF 类型，因此允许定义 4 种不同的通信量规范概要。用户可以选择一个或多个类来满足需求。在每个类中，分组被客户或服务提供者标以三种丢弃优先级中的一种。在遇到拥塞时，分组的丢弃优先级决定该 AF 类中分组的相对重要性。拥塞的 DS 节点试图保护具有较低丢弃优先级的分组免于丢弃，其手段是先丢弃具有较高丢弃优先级的分组。

3）其他服务类型

在 DiffServ 体系中，服务类型与实现它的 PHB 在定义上是相互分离的。这种处理主要是基于灵活性的考虑：服务类型可能因 ISP 而异，而且发展变化较快，但实现模块 PHB 却相对保持稳定。因此 IETF 的标准化工作仅仅针对 PHB，而服务类型则是完全开放的，由各 ISP 自行确定。

同一 PHB 通过与不同的边界分类调节机制相结合，可以实现不同的服务。例如，AF 也可以用来实现优于尽力而为服务（Better than Best-Effort service，BBE）和定量确保的多媒体播放服务（quantitative assured media playback service）等。如果新的服务类

型无法用已有 PHB 实现，就需要定义新的 PHB。

1.10.3 MPLS QoS 技术

1．MPLS 的背景

20 世纪 80 年代，随着因特网的迅速发展，人们开始探索如何提高分组转发速度的方法。这时出现了一种思路：用面向连接的方式取代 IP 的无连接分组的交换方式，这样就可以利用更快捷的查找算法，而不必使用最长前缀匹配的方法来查找路由表。这种基本概念就叫做交换（switching）。

为了实现交换，可以利用面向连接的概念，使每个分组携带一个叫做标记（label）的小整数（也就是给分组打上一个标记）。当分组到达交换机（即标记交换路由器）时，交换机读取分组的标记，并用标记值来检索分组转发表。图 1-144 描述了这一概念。

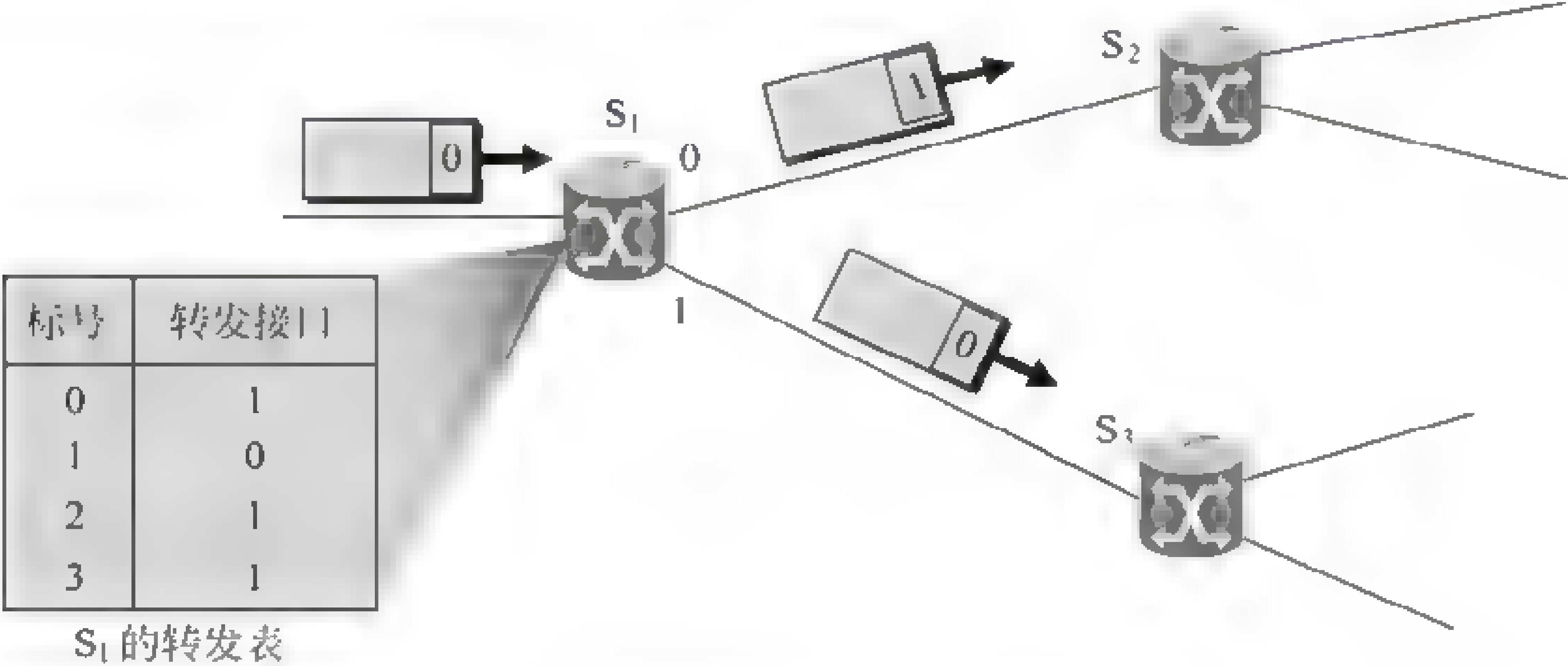


图 1-144 交换机根据分组的标记转发分组

图 1-144 画出了交换机 S_1 中已建立的分组转发表。每个进入交换机的分组都携带一个标记。图中画出了携带标记 0 的分组从 S_1 的接口 1 转发出去，而携带标记 1 的分组则从 S_1 的接口 0 转发出去。这样的转发速度要比查找路由器快得多。

按照以上思路，IETF 于 1997 年成立了 MPLS 工作组，以便开发出一种新的协议标准。这种新的协议取名为多协议标记交换（Multi-Protocol Label Switching，MPLS）。“多协议”表示在 MPLS 的上面可以采用多种协议。IETF 还综合了许多公司的类似技术，如 Cisco 公司的标记交换 TAG（TAG switching），以及 Ipsilon 公司的 IP 交换（IP switching）等。2001 年 1 月 MPLS 终于成为因特网的建议标准（RFC 3031，3032）（W-MPLS）。

现在 MPLS 受到网络界人士的高度重视，因为 MPLS 具有以下 4 个方面的特点：

（1）支持面向连接的服务质量。

（2）支持流量工程，平衡网络负载。

（3）有效地支持虚拟专用网（VPN）。

（4）支持多种网络协议。

2．MPLS 的工作原理

1）基本工作过程

在传统的 IP 网络中，分组每到达一个路由器，都必须查找路由表，并按照“最长前缀匹配”的原则找到下一跳的 IP 地址（请注意，前缀的长度是不确定的）。当网络很大时，查找含有大量项目的路由表要花费很多的时间。在出现突发性的通信量时，往往还会使缓冲溢出，这就会引起分组丢失、传输时延增大和服务质量下降。

MPLS 的一个重要特点就是不用长度可变的 IP 地址前缀来查找转发表中的匹配项目，而是给每一个 IP 数据报打上固定长度“标记”，然后对打上标记的 IP 数据报用硬件进行转发，这就使得 IP 数据报转发的过程省去了每到达一个路由器都要上升到第三层用软件查找路由表的过程，因而 IP 数据报转发的速率就大大地加快了。采用硬件技术对打上标记的 IP 数据报进行转发就称为标记交换。“交换”也表示在转发时不再上升到第三层查找转发表，而是根据标记在第二层用硬件进行转发。MPLS 可使用多种链路层协议，如 PPP、以太网、ATM 以及帧中继等。图 1-145 是 MPLS 协议的基本原理的示意图。

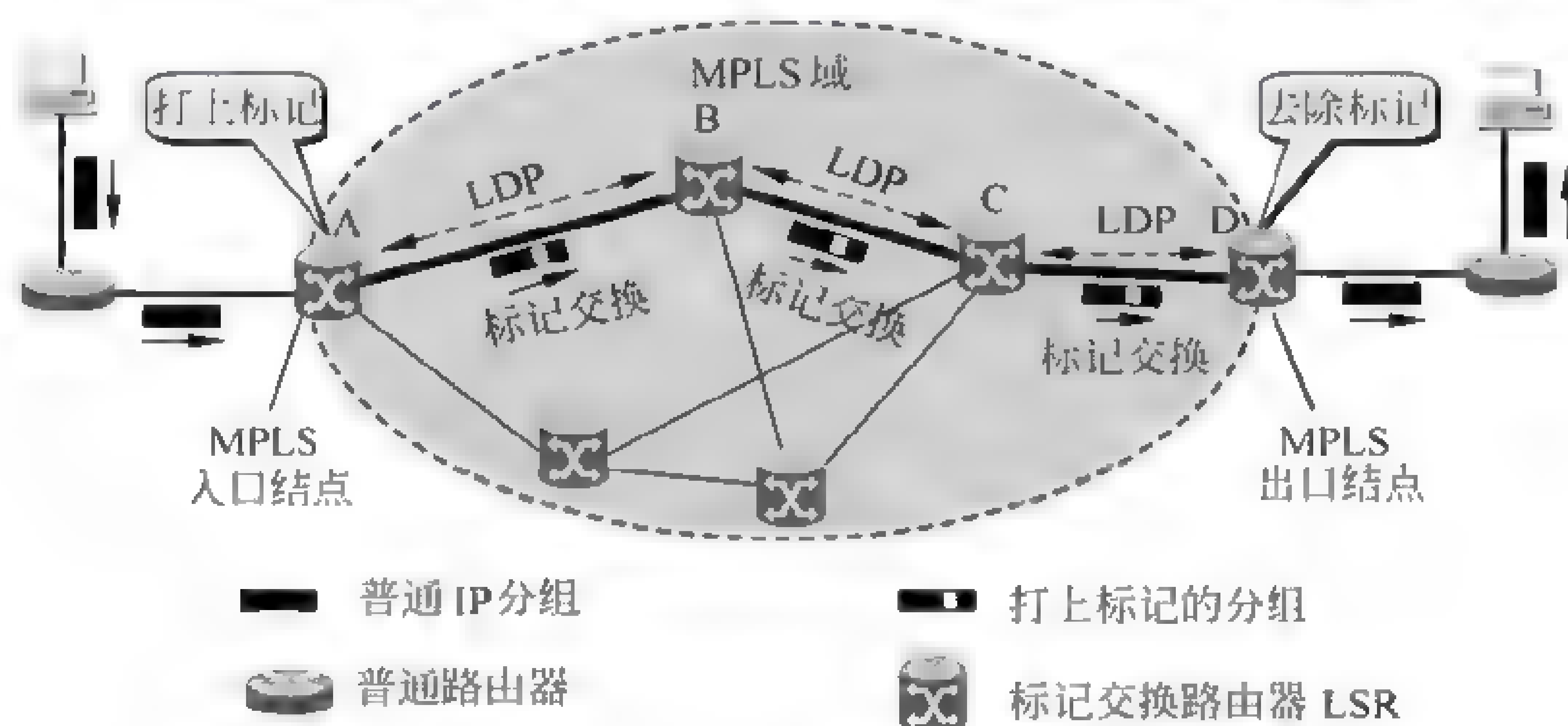


图 1-145　MPLS 协议的基本原理

MPLS 域（MPLS domain）是指该域中有许多彼此相邻的路由器，并且所有的路由器都是支持 MPLS 技术的标记交换路由器（Label Switching Router，LSR）。LSR 同时具有标记交换和路由选择这两种功能，标记交换功能是为了快速转发，但在这之前 LSR 需要使用路由选择功能构造转发表。

图 1-145 中给出了 MPLS 的基本工作过程如下。

（1）MPLS 域中的各 LSR 使用专门的标记分配协议（Label Distribution Protocol，LDP）交换报文，并找出和特定标记相对换的路径，即标记交换路径（Label Switched Path，LSP）。例如在图中的路径 A→B→C→D。各 LSR 根据这些路径构造出转发表。这个过程和路由器构造自己的路由表相似（RFC 3031）。但应注意的是，MPLS 是面向连接的，因为在标记交换路径 LSP 上的第一个 LSR 就根据 IP 数据报的初始标记确定了整个的标记交换路径，就像一条虚连接一样。

（2）当一个 IP 数据报进入到 MPLS 域时，MPLS 入口节点（ingress node）就给它打上标记（后面我们就会知道，这实际上是插入一个 MPLS 首部），并按照转发表把它转发给下一个 LSR。以后的所有 LSR 都按照标记进行转发。

给 IP 数据报打标记的过程叫做分类（classification）。严格的第三层分类是只使用了 IP 首部中的字段，如源 IP 地址和目的 IP 地址等。大多数运营商实现了第四层分类（除了要检查 IP 首部外，还要检查 TCP 或 UDP 首部中的协议端口号），而有些运营商则实现了第五层分类（更进一步地检查数据报的内部并考虑其有效载荷）。

（3）由于在全国内统一分配全局标记数值是非常困难的，因此一个标记仅仅在两个标记交换路由器 LSR 之间才有意义。分组每经过一个 LSR，LSR 就是要做两件事。一是转发，二是更新的标记，即把入标记更换成为出标记。这就叫标记对换（label swapping）。做这两件事所需的数据都已清楚地写在转发表中。例如，图 1-145 中的标记交换路由器 B 从入接口 0 收到一个入标记为 3 的 IP 数据报。查找转发表见表 1-20。标记交换路由器 B 就知道应当把该 IP 数据报从出接口 1 转发出去，同时把标记对换为 1。

表 1-20　标记交换路由器转发表

入接口	入标记	出接口	出标记
0	3	1	1

当 IP 数据报进入下一个 LSR 时，这时的入标记就是刚才得到的出标记。因此，标记交换路由器 C 接着在转发该 IP 数据报时，又把入标记 1 对换为出标记 2。

（4）当 IP 数据报离开 MPLS 域时，MPLS 出口节点（egress node）就把 MPLS 的标记去除，把 IP 数据报交付给非 MPLS 的主机或路由器，以后就按照普通的转发方法进行转发。

上述的这种“由入口 LSR 确定进入 MPLS 域以后的转发路径”称为显式路由选择（explicit routing），它和因特网中通常使用的“每一个路由器逐跳进行路由选择”有着很大的区别。

2）转发等价类（FEC）

MPLS 有个很重要的概念就是转发等价类（Forwarding Equivalence Class，FEC）。所谓“转发等价类”就是路由器按照同样方式对待的 IP 数据报的集合。这里“按照同样方式对待”表示从同样接口转发到同样的下一跳地址，并且具有同样服务类别和同样丢弃优先级等。FEC 的例子是：

① 目的 IP 地址与某一个特定 IP 地址的前缀匹配的 IP 数据报（这就相当于普通的 IP 路由器）。

② 所有源地址与目的地址都相同的 IP 数据报。

③ 具有某种服务质量需求的 IP 数据报。

总之，划分 FEC 的方法不受任何限制，这都由网络管理员来控制，因此非常灵活。入口节点并不是给每一个 IP 数据报指派一个不同的标记，而是将属于同样 FEC 的 IP 数据报都指派同样的标记。FEC 和标记是一一对应的关系。

显然，FEC 可以有不同的粒度。细粒度的例子是为特定源主机和目的主机之间的特定应用指派的 FEC。与特定出口 LSR（不管数据流是从哪一个源节点发送过来的）相关联的 FEC 则是粗粒度的例子。在这种情况下许多应用流聚合到出口 LSR 离开 MPLS 域，像一棵倒置的树，它的根在出口 LSR。这种应用流的聚合也称为虚电路合并（VC merging）。这样做可以大大减少转发表中的项目数。图 1-146 给出了一个例子。这个图表示，进入一个 LSR 的不同入标记的 IP 数据报，在离开 LSR 时都具有相同的出标记，因为它们都是要到达同一个出口 LSR 的。例如，进入标记交换路由器 S_1 的 IP 数据报，不同的入标记 1 和 3，都对换成相同的出标记 2。而进入标记交换路由器 S_3 的 IP 数据报，不同的入标记 1 和 2，都对换成相同的出标记 4。

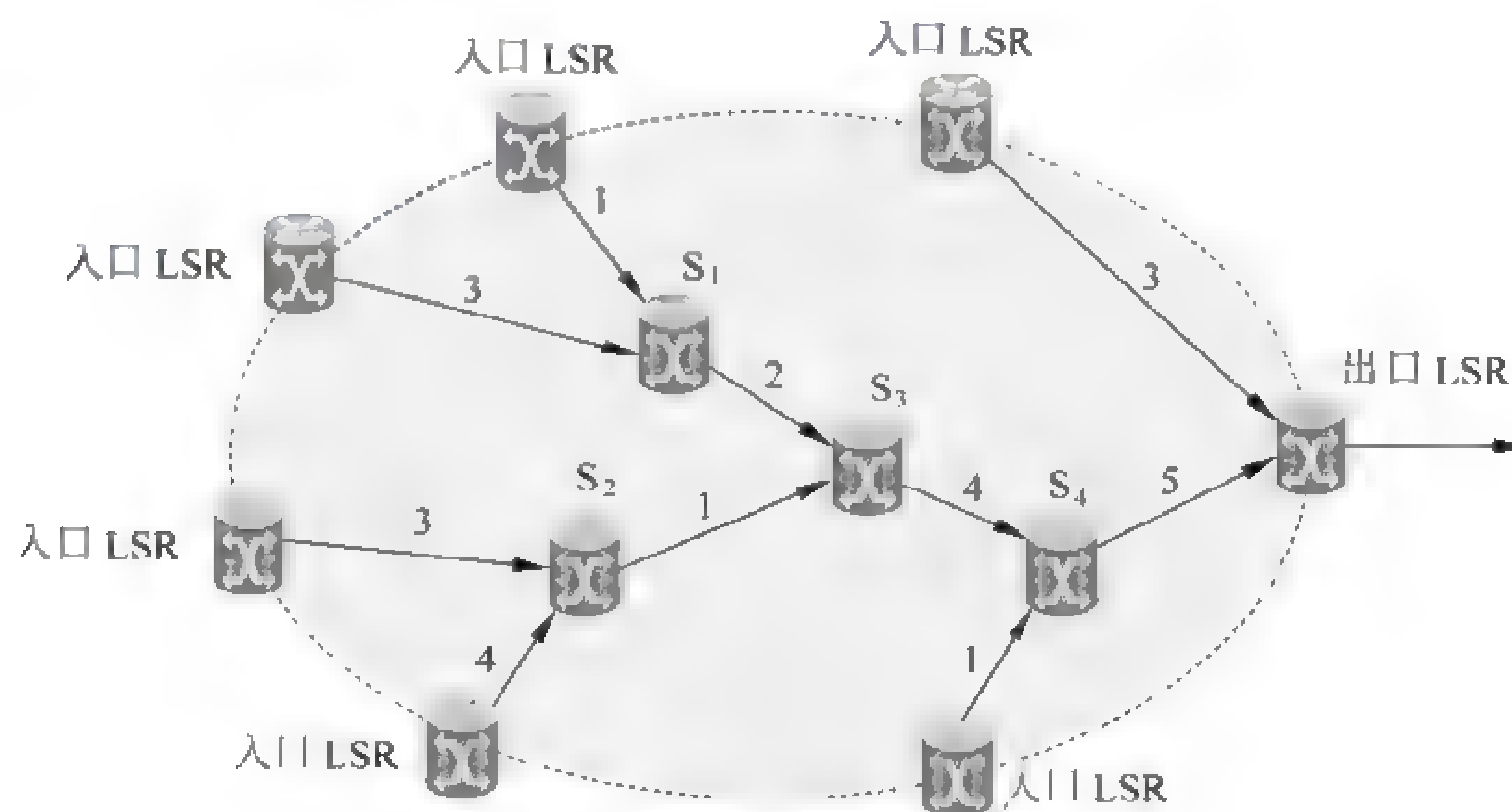


图 1-146　应用流聚合到出口 LSR

图 1-147 给出一个把 FEC 用于负载平衡的例子。图 1-147（a）的主机 H_1 和 H_2 分别向 H_3 和 H_4 发送大量数据。路由器 A 和 C 是数据传输必须经过的。但传统的路由选择协议只能选择最短路径 A→B→C，这就可能导致这段最短路径过载。

图 1-147（b）表示在 MPLS 的情况下，入口节点 A 可设置两种 FEC：“源地址为 H_1 而目的地址为 H_3” 和 “源地址为 H_2 而目的地址为 H_4”，把前一种 FEC 的路径设置为 H_1→A→B→C→H_3，而后一种的路径设置为 H_2→A→D→E→C→H_4。这样可使网络的负载较为平衡。网络管理员采用自定义的 FEC 就可以更好地管理网络的资源。这种均衡网络负载的做法也称为流量工程（traffic engineering）或通信量工程。

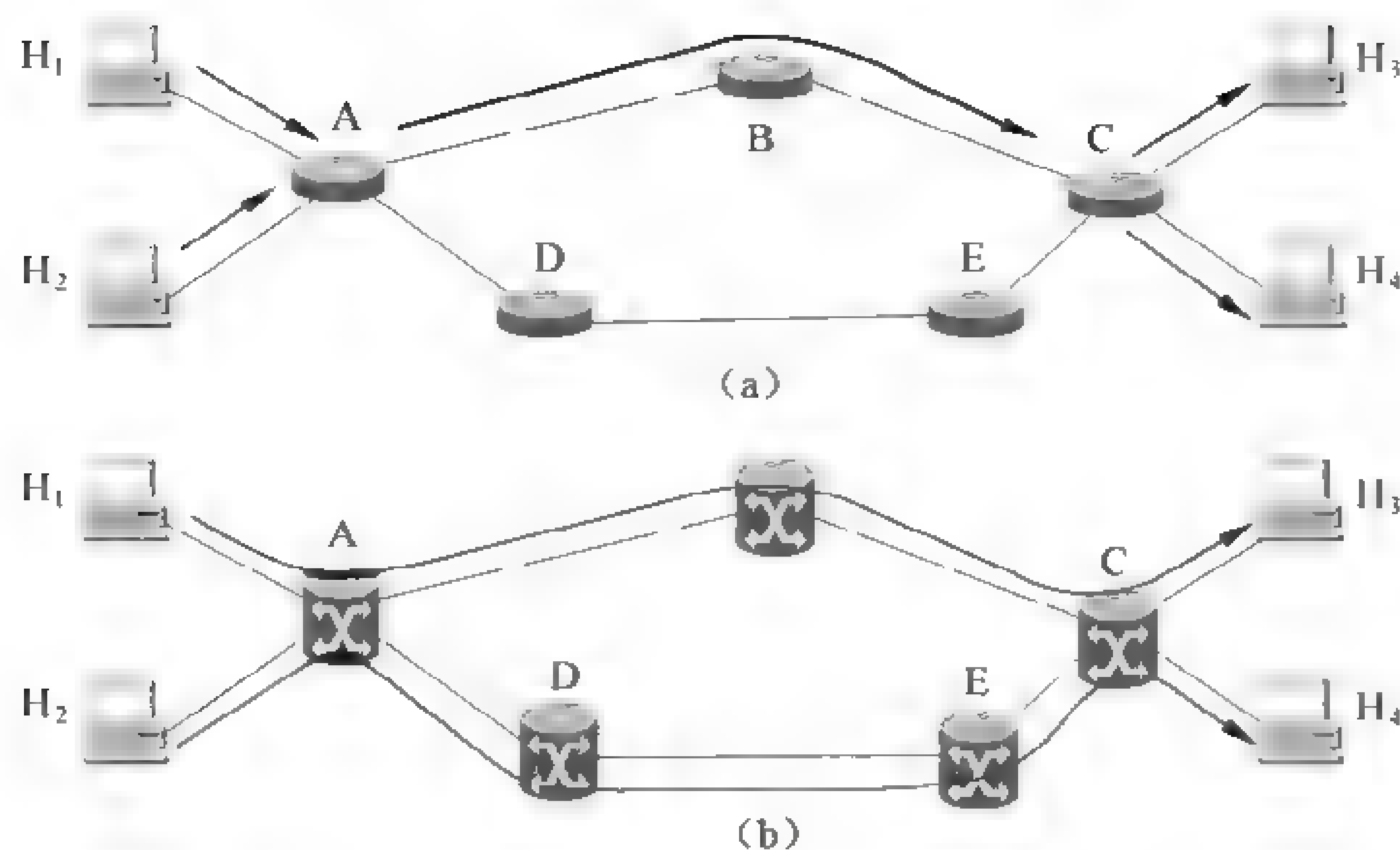


图 1-147 FEC 用于负载平衡

1.10.4 移动网络 QoS 技术

移动互联网的拓扑结构和资源都在动态地变化，要提供服务质量保证比固定网更为困难。目前，根据无线和移动环境的特点，人们对原有的 QoS 技术进行了改进。

1．移动环境下的 IntServ 和 RSVP

目前的 RSVP 不适合于移动 IP 网络，主要原因是它无法感知主机的移动，因而不能在移动主机即将访问的位置上提前预留资源，当主机移动到新的子网后往往因缺乏资源而导致服务质量下降。另外，目前的 RSVP 不支持经过 IP 隧道的资源预留，因此不能适应移动 IP 网利用隧道传送数据时的服务质量要求。为了克服 RSVP 的缺陷，提出了以下 4 种解决方案：

1）MRSVP

MRSVP 协议要求预测主机未来可能到达的位置，并在这些位置中提前预留资源。在 RSVP 中有主动和被动两种资源预留方式，主动资源预留用于移动主机当前所在的子网，被动资源预留用于未来访问的子网。被动预留的资源可以被子网中其他业务流使用，但当移动主机移动到该子网时，子网中被动预留的资源即转变为主动预留资源，供移动主机使用，而原来使用这些资源的业务流需要立刻释放所占用的资源。

2）支持隧道的 RSVP

支持隧道的 RSVP 建议在隧道的两个端点之间为通过隧道的总业务量预留资源。这样，在端到端的 RSVP 会话经过隧道时，就没有必要再考虑隧道中的资源预留。

3）基于组播的 RSVP

在基于组播的 RSVP 协议中，每个移动主机用一个组播地址来标识，所有移动主机在发送、接收 RSVP 消息和 IP 数据包时都通过组播方式进行，主机的移动可视为组播组

成员的变动。该方案还采用了类似于 MRSVP 的运动预测机制，由移动代理将移动主机下一步将要访问的位置提前加入到组播树中，并预留资源。另一方面，用剪枝的方法将主机已经离开的位置从树上删除。

4）DRSVP

DRSVP 是一种支持可变服务质量的动态资源预留协议，它使用户能够根据网络资源的变化动态调整服务质量要求。DRSVP 的主要做法是在 Resv 消息中增加参数来描述业务流的适应范围，通报上、下游的资源“瓶颈”，并引入新的带宽分配算法，以适应网络资源的动态变化。这个方案的优点是允许预留的资源有一个波动范围，从而灵活地支持服务质量需求，并使网络资源利用率也得到提高。

2．移动环境下的 DiffServ

目前的 DiffServ 不能满足移动 IP 网的要求，主要原因有两个：一是没有信令，不能做到实时控制；另一个原因是不能动态配置服务质量参数。

无线环境下的 DiffServ 框架，对 DiffServ 的功能进行了以下扩展：

- 增加信令协议，用于在移动终端和基站之间传送控制消息及相关参数（如移动终端的能量、当前的丢失率等）。
- 增加对移动性的支持，为移动主机预留带宽，或者赋予移动主机高优先级，使其在切换时能够抢占低优先级业务的带宽，或使用预留带宽来补偿无线链路的高误码损失。
- 要求基站能够过滤掉部分不重要的信息，以解决有线和无线链路速率不匹配的问题，或减少终端的能耗。

移动环境下的 QoS 策略，其发展趋势如下：核心网采用 DiffServ，无线接入网既可采用 IntServ 也可采用 DiffServ；无线接入网内用信令协议支持动态资源分配；资源分配信令可以和移动主机位置管理信令相结合，以加快资源分配过程，减少信令开销。另外，动态资源分配可以同接纳控制和无线分组调度等技术结合，更好地解决 QoS 问题。

3．移动 IPv6 服务质量

当移动节点改变网络连接点时，数据包经过的中间网络域可能发生变化。因此，在这些网络域中，需要在移动节点的数据包上提供适当的服务质量支持，这样运行在移动节点上的服务质量敏感应用程序能保持可用的服务等级。

1）基于 RSVP 的移动 IPv6 服务质量体系

有的方法提出了一个无线和移动网络中的信令协议，当移动主机从一个子网移动到另一个子网时，允许移动主机在当前位置的路径上建立和维持预留资源。这个协议通过结合 RSVP 隧道和移动 IP 协议来实现。

有的方法解决了在移动 IP 网络中运行 RSVP 信令的问题，采用优化路由，讨论了基本解决方法：在移动节点和通信节点上修改 RSVP，使其知道移动 IPv6 的地址；允许在固定和移动网络之间传输 RSVP 数据流。

上述这些为移动用户提供服务的方法都是基于 RSVP 的，因此就有了 RSVP 的可扩展性问题。例如，现有的资源预留协议的设计着眼于由静止主机构成的网络，为了支持移动环境的资源预留，还应对 RSVP 协议进行扩展和修改，使其支持移动节点（MN）的资源预留。另一种方法是定义特别的 IPv6 扩展头标作为资源预留信令，这样可在一个分组中综合 QoS 信息、地址绑定信息和 IPv6 数据分组，节约信令开销。对移动 IPv6 节点发送的分组中可根据其本地地址和流标记来识别一个数据流，但需要各边缘路由器支持移动 IPv6 的本地地址信宿选项。IP 移动性和 RSVP 时结合是很复杂的问题。

2）基于区分服务的移动 IPv6 服务质量体系

有些学者提出了一个移动 IPv6 网络的服务质量结构框架。该结构是基于区分服务的，因为数据流是以集合的方式在主干网上传输的。每个管理域中至少有一个全局服务器，称为全局服务质量代理（GQA），有几个归属节点作为归属服务质量代理（LQA）。这种结构的主要特点是：GQA 是在控制面上，LQA 是在传输面上。由于在中心服务器上保留全局信息，并且将控制和数据传输分开，这个结构用于移动环境时非常灵活，易于添加新的服务，并且更加有效。GQA 和 LQA 之间的通信采用 COPS（Common Open Policy Service）。该结构还考虑了集成移动 IPv6 和区分服务的其他问题，如移动环境下的网络资源提供、缺乏动态配置问题、服务等级约定的定义和选择、移动数据流的标识和计费等。

在移动 IP 中实现 QoS 要比在固定 IP 网络中复杂得多。区分服务用于移动 IP 中存在以下问题：

- 区分服务比较适用于设计周全、带宽合理分配的网络，支持移动环境的网络由于其网络中的节点随时移动，因而其业务量模型比较复杂。
- 在区分服务中，不同 QoS 区域（如不同的 ISP 提供的网络）的业务等级协议（SLA）常常是静态的，移动 IP 的高动态环境与区分服务的静态带宽分配是相矛盾的，因此为了 MN 的动态带宽分配需要，必须支持动态的业务等级协商。
- 在不同 QoS 区域的入口处，网络的边缘路由器要对分组流进行识别，传统分组流可以通过分组头标上的五元组（源/目的 IP 地址、协议类型、源/目的端口号）来识别。而移动 IPv6 中的分组的源 IP 地址（MN 发送的分组）或目的 IP 地址（MN 接收的分组）是 MN 的转交地址，该地址随着节点的移动而动态地变化。

为了在移动 IP 网络上实现区分服务，应精细设计提供移动服务的网络，动态预测移动节点对带宽的需求和接入的 MN 数，或采用资源预留等信令机制，更准确地预测满足移动节点 QoS 所需的带宽。

3）服务质量对象

在某些方法中，引入了一个新的 IPv6 选项，称为“服务质量对象”。根据上下文的不同，服务质量对象可以作为目的选项或者 Hop-by-Hop 选项，包含在绑定更新和绑定认可消息中。作为 Hop-by-Hop 选项时，服务质量对象在中间网络域触发特定的服务质

量过程。

这些方法的基本思想是把服务质量对象作为 Hop-by-Hop 选项放在绑定消息中，传输方向与服务质量敏感的数据流相同（本地代理 HA 到 MN、核心网 CN 到 MN 或者 MN 到 CN）。当数据包在端到端路径上穿过不同域时，需要检查服务质量对象，为 MN 的数据包提供服务质量支持。

4）移动服务质量其他问题

MN 在越区切换时引入的分组传输延时和分组丢失也是移动 IP 急需解决的问题，这个问题不解决，移动 Internet 的 QoS 保证就无从谈起。缓存管理可以使得切换更为平滑。具有缓存管理功能的路由器，在路由器通告消息中向感兴趣的移动节点通告它的缓存能力。当移动节点收到指示后可以获得缓存服务的路由器通告时，它可以使用定义的缓存初始化子选项请求缓存。移动节点可以请求确定的缓存空间或者接受默认的缓存空间；路由器根据可用资源，可以接受或拒绝此请求，或者根据需要分配一个更小的缓存，其大小通过定义的缓存确认子选项通知移动节点。

第 2 章　计算机网络规划与设计

2.1　设计基础

2.1.1　网络基本元素

计算机网络由多种基本元素组合而成，常见的网络基本元素包括计算机平台、应用软件、物理设备和拓扑结构、网络软件和实用软件、互联设备和广域网连接等。

在不同的计算机网络中，设计者通过不同基本元素的组合，形成了不同规模、满足不同应用需求的网络。

1．计算机平台

计算机平台是网络中的终端用户节点，是装载并运行操作系统和应用程序并为用户提供功能和服务的设备，不同的计算机平台，其形状、尺寸、性能有所不同。按照功能的不同，可以将计算机网络中的计算机平台简单划分为计算机终端、网络计算机（NC）、个人计算机、工作站、小型服务器、大型服务器。

在进行计算机网络设计时，各类计算机平台的微处理器的类型、内存、输入输出、操作系统、设备驱动器、存储器等都将对设计工作产生影响。例如在一个电子图书阅览室内部局域网设计中，如果所有阅览计算机都采用网络计算机，由于该类平台本身不具备硬盘等存储设备，实际上是通过远程访问中心服务器来完成阅读工作的，因此对局域网的带宽、中心服务器的性能要求就不同于所有阅览机采用个人计算机的网络规划方案。

2．应用软件

应用软件运行于计算机平台之上，是完成某种特定应用的软件系统，是网络系统中常用的软件之一。应用软件分为多种类型，如有些应用软件运行在单机模式中，而另外一些则运行在多机模式中，需要网络环境的支持。由于应用软件直接体现了用户的应用需求，因此网络设计工作必须考虑应用软件的使用方式和需求，以便于保证应用软件的整体性能。例如，一个企业网络的互联网出口既承载着企业大量内部数据对互联网发布的应用，同时又是内部人员访问互联网的基础，在设计中必须考虑到对内部人员访问互联网络进行流量控制，否则大量的 P2P 访问流量就会导致出口带宽被占用，严重影响企业业务数据发布的功能。又例如，对于一个核心企业应用系统来说，采用 C/S 架构和 B/S 架构，对核心服务器、网络带宽的要求是不同的，应根据用户的需求进行相应的网络

设计。

应用软件也会影响用户对网络和系统的感觉。如果用户借助设计不佳的网络，在一个速度极慢的计算机上运行过时的应用软件，用户将不会喜欢这样的系统。因此，在网络设计中应选择适合所设计的网络环境的应用软件。

3．物理设备和拓扑结构

物理设备是指连接网络端点之间的基础设施，如网卡、电缆、接插件、接插板、集线器等，而一个网络，是由各种各样的物理设备连接而构成的。在设计一个网络时，电缆类型、物理设施允许的速率、网络设备的位置和类型都起着重要的作用。

网络拓扑结构是指在给定终端位置的情况下网络的结构方式。拓扑结构决定了网络的工作原理及网络信息的传输方式。一旦确定了网络的拓扑结构，就要选择适合这种拓扑结构的工作方式与信息的传输方式。如果选择和配置不当，将影响网络安全。

常见的网络拓扑结构分为两大类，分别是广域网拓扑结构和局域网拓扑结构。其中广域网拓扑结构有集中式、分散式、分布式、不规则式等结构，局域网拓扑结构有星状结构、环状结构、总线结构、树状结构和网状结构等。在实际应用中，通常是由它们组成的混合形式，而非单一的拓扑结构。

4．网络软件和实用软件

在设计、运行和维护网络的过程中，网络软件和实用软件占有非常重要的地位。其中网络软件主要由客户机端的软件和客户机之间或客户机与服务器之间进行通信所需要的协议堆栈支撑软件组成。由于网络软件负责实现网络中的协议传递、服务提供，并由此产生网络上的各种协议流量，因此在网络设计中，如何选择合适的网络软件是需要重点考虑的问题。在网络软件和应用软件的区别上，需要说明的是网络软件是为底层协议服务的通用软件，而应用软件是为实现业务流程服务的特殊软件。

实用软件主要是用于实现网络分析、管理、监控、维护、故障发现排除等功能，而专门为网络定制的特殊软件，既包括网络管理软件，例如，惠普公司的 OpenView 以及 Sun 公司的 SNM 之类的复杂软件，又包括像 ping、traceroute 之类的简单软件。

5．互联设备

在不同类型的网络间进行通信时，需要使用各种互联设备来实现异构网络间的协议转换、同构网络间的网络范围延伸。网络互联设备包括网桥、交换机、路由器、网关等，通过这些设备形成网络的框架，并用来提高网络性能。

在网络设计中，网络互联设备的选择十分重要。在不同的互联层次，应选择不同的互联设备。例如，如果在第二层实现异构网络互联，选择网桥；在第二层实现以太同构互联，则选择以太交换机；在第三层实现网络连通，选择路由器。不同层次的互联设备不仅实现互联的原理不同，同时也会对网络的性能、可维护性、可扩展性产生不同的影响。

6．广域网连接

广域网连接使局域网（LAN）和校园网转变成城域网（MAN）和广域网（WAN），广域网连接采用点对点还是交换式、高速还是低速都将直接影响到网络的性能和效率。

广域网连接设计也是网络设计中非常关键的一步，因为大部分的网络费用是用于租用公共服务和设施的。而广域网的连接是利用这种潜在而且昂贵的资源，因此必须认真考虑网络应用和用户服务需求。

2.1.2 网络互联设备

随着网络技术的不断发展，为了满足人们对网络环境、应用、性能价格比的不同要求，多种网络互联设备应运而生，使网络设计的内容更为丰富。这些互联设备工作在不同的网络层次，通过不同原理实现网络互联，具有不同的优缺点，如表 2-1 所示。

表 2-1 互联的层次性

实现互联层次	实 现 原 理	优 点	缺 点
物理层	信号复制与放大	错误分隔、互联方便简洁	互联网络必须同构，互联范围狭小
链路层	数据帧存储转发	数据帧过滤，安全性提高，异构网络互联	无法屏蔽网络风暴，网络规模过大时网络性能降低
网络层	分组存储转发	防止网络风暴、自动寻径、中间节点差错控制、流量控制	易成为网络瓶颈，网络资源共享度降低
传输层以上	协议转换	互联层次高，与用户信息直接接触	服务专用性强，应用范围狭窄，效率低

网络互联设备主要包括中继器、集线器、网桥、交换机、路由器、网关等，各种互联设备工作的层次、工作原理、实现方式如图 2-1 所示。

1．中继器

中继器是最简单的互联设备，它的作用是放大电信号，扩大网络的地理覆盖范围。中继器工作在 ISO 的最低层——物理层，它可以使介质错误仅局限于一段网络内，而不会对其他段造成影响。

中继器只使用在早期基于总线型的局域网络内，主要使用的介质是粗同轴电缆或细同轴电缆，并且在综合布线中大量使用中继器进行水平互连。

2．集线器

集线器（hub）是局域网内连接服务器与主机的主要设备，工作在 OSI 参考模型的物理层，有信号放大作用。

从局域网络拓扑结构来看，集线器的出现使得早期不稳定的总线型网络被星型网络所替代，集线器的使用如图 2-2 所示。集线器类似于一根被压缩于一个点的总线，与总

线相比具有信号放大的功能。

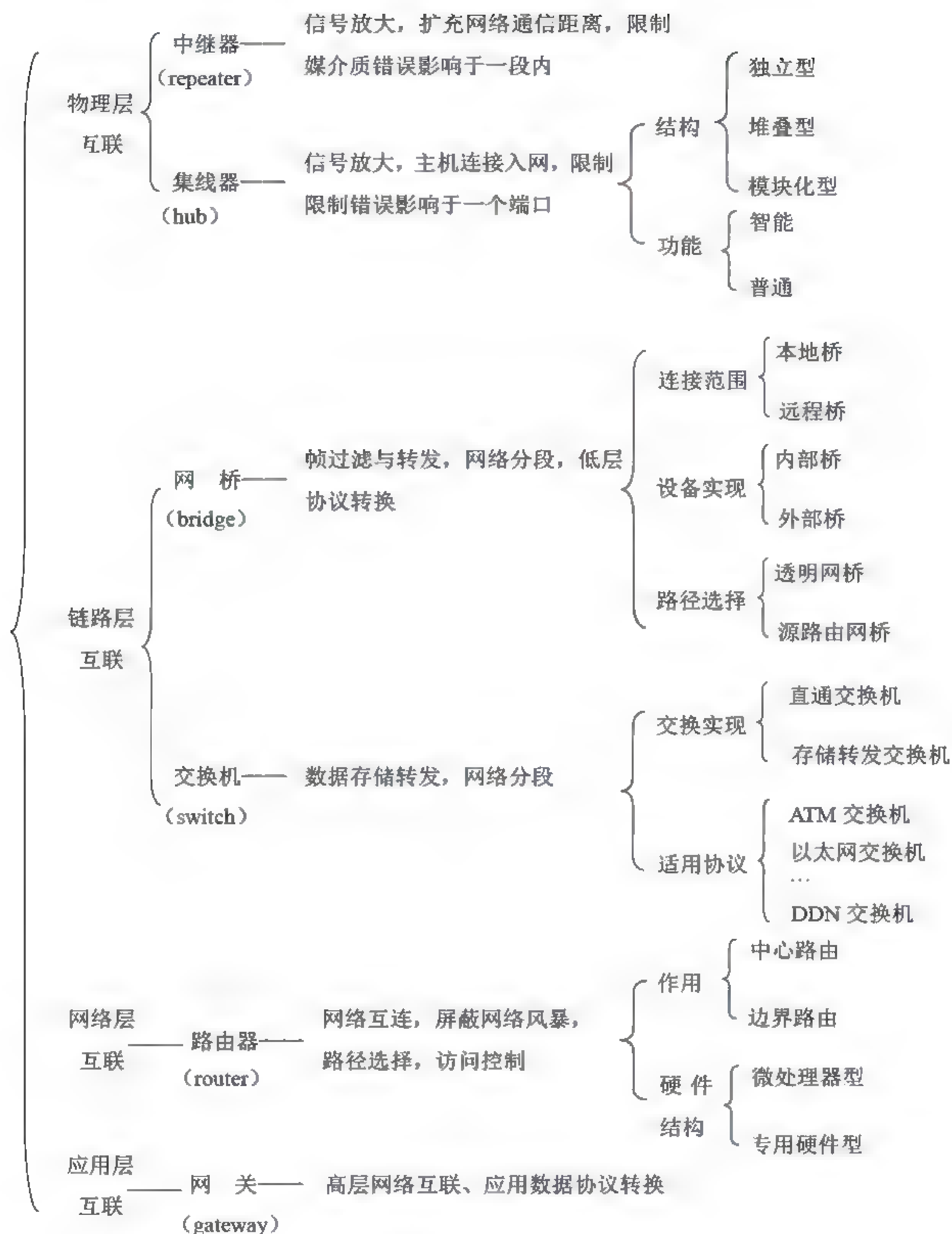


图 2-1　互联设备分类

3．网桥

网桥是一种在数据链路层实现互联的设备，在网段之间进行数据帧的接收、存储与转发。数据链路层分为逻辑链路控制子层（LLC）和媒体访问控制子层（MAC）两部分，

LLC 用于子网间路径选择，MAC 用于介质访问以及数据帧的成帧等处理。网桥互联的网络可以是异构网络，其异构性表现为相同的逻辑链路控制子层而媒体访问控制子层不一致。网桥的作用主要是异构局域网络互联、数据帧转发、路径选择等，在早期的网络互联中是增加网络跨度的主要手段，在现代网络中已逐步被网络交换机所代替。

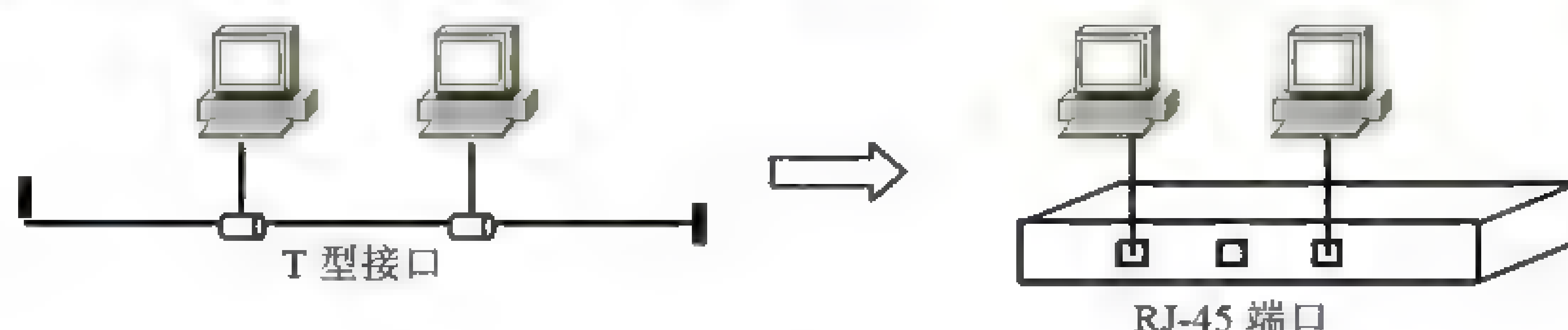


图 2-2 集线器使用示意图

网桥按连接范围分为本地桥和远程桥，按实现方式分为内部桥和外部桥，根据路径选择方法分为透明网桥和源路由网桥。在这三种分类方式中，按路径选择方法进行分类的意义较大，不同类网桥的原理及实现方法不同。

透明网桥不允许冗余桥设备出现，具有自学习功能，可以根据学习到的 MAC 地址分布情况进行数据帧转发，在网络互联时，通过生成树算法避免网桥环路的出现。源路由网桥是指在帧内包含了帧的路由信息，从而使网桥根据路由信息进行帧转发，而路由信息则是依据侦测数据帧进行广播后目标主机响应的最优路径产生。

4．以太网交换机

随着网络的不断发展，网络用户的不断增加，共享总线型局域网内用户数量激增，冲突发生频率增加，单个用户可用带宽减少，网络效率降低。随之产生的解决方法称为“网络微化”，就是将一个共享型局域网切割为多个微型局域网段，网段之间通过桥接或路由互连，其实质在于将广播域划分为多个冲突域，这样网络成本增加，互连设备成为网络瓶颈。网络进一步发展时，每一个段内很快又增加了大量用户，使得微化后的段内又开始出现相同的情况，因此，网络微化不是最终解决方法，而交换或局域网的出现才是这一类问题的最好解决方法。

交换式网络在现有的情况下，主要是通过交换式设备——以太网交换机来实现互连。以集线器互连与以交换机互连的区别如图 2-3 所示。

交换机是一种存储转发设备，与原有的桥接器相比较，交换机每一个端口的承载能力相当于桥接器上的一段。交换机工作在 ISO 的第二层，根据发送帧中的目标 MAC 地址进行转发，在交换机的内部维护着 MAC 地址表，指明某一个 MAC 地址归属于哪一个端口，帧从源主机到目标主机的转发在交换机内部实际上是由可以识别源主机 MAC 地址的端口与识别目标主机 MAC 地址的端口之间的帧转发实现的。

交换机的信息转发有两种主要的实现方式：直通方式与存储转发。直通方式主要通过内部交换矩阵实现，在接收到帧的源地址、目标地址后，查找内部 MAC 地址表，进

行帧的转发。存储转发方式是借助于交换机内部的高速缓冲，所有接收到的帧都存入该缓冲区中，在转发时由缓冲区进行输出。存储转发方式的时延较大，但是由于其特殊的处理方式，可以进行帧校验、帧过滤等功能的实现，相对于直通方式，存储转发交换机提供的功能要强大得多，尤其是大多数交换机都支持的虚拟网络功能，只能在存储转发式交换机上实现。

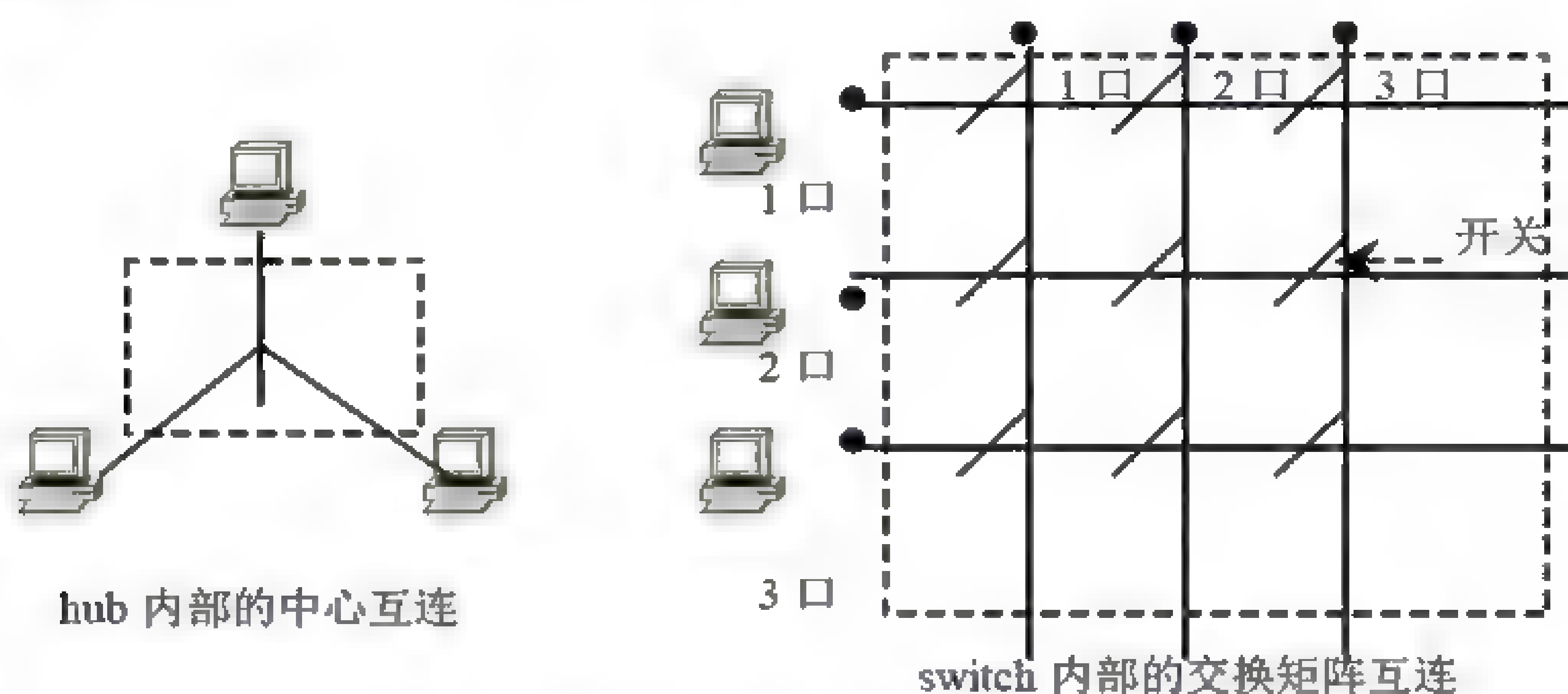


图 2-3　集线器互联与交换机互联的区别

关于交换机，一般运用在网络主干上，特指高速传输主干，在现行网络条件下，网络主干传输率多在 1000Mbps 以上，100Mbps 的交换设备已经逐步演变成为桌面级设备，也就是现在较为流行的“百兆交换到桌面”。虚拟网络是现代交换机屏蔽网络风暴的一种方式，交换机将一个大的广播域划分为几个小网段，每一个网段就是逻辑上的独立广播域，网段之间的通信必须通过三层设备——路由器进行互联，虚拟网络是目前突破网络地理局限性的较好方式。

5. 路由器

路由器是工作在网络层的互联设备，是可以屏蔽网络广播风暴的有效网络设备。路由器的功能较多，如图 2-4 所示。

目前路由器上所运行的路由算法较为复杂，种类繁多，一般来说，路由算法主要使用两种算法，分别是静态路由算法与动态路由算法，如图 2-5 所示，其中动态路由算法又分为矢量路径算法、链路状态算法与层次型算法。无论是静态路由还是动态路由，最本质的目的都是在维护一张路由表，在数据包到来时，查找路由表，找到最为匹配的路由信息而决定数据包的路由。动态路由的优点是可以根据网络的当前状态（互连情况、拥塞情况等）自动修改路由信息，动态路由算法都有 4 个阶段：测量→报告→更新→决策，该类算法定期测量相关的网络参数，并且向参与算法的路由器进行报告，各路由器根据参数自动进行路由表更新，而决策是指数据包根据路由表进行路由选择的过程。

现代路由产品一般分为两大类，一类是用于网络外围，实现园区网络与外界互联的边界路由器；另一类是用于园区网络内部各子网之间互联及信息传递的中心路由器。

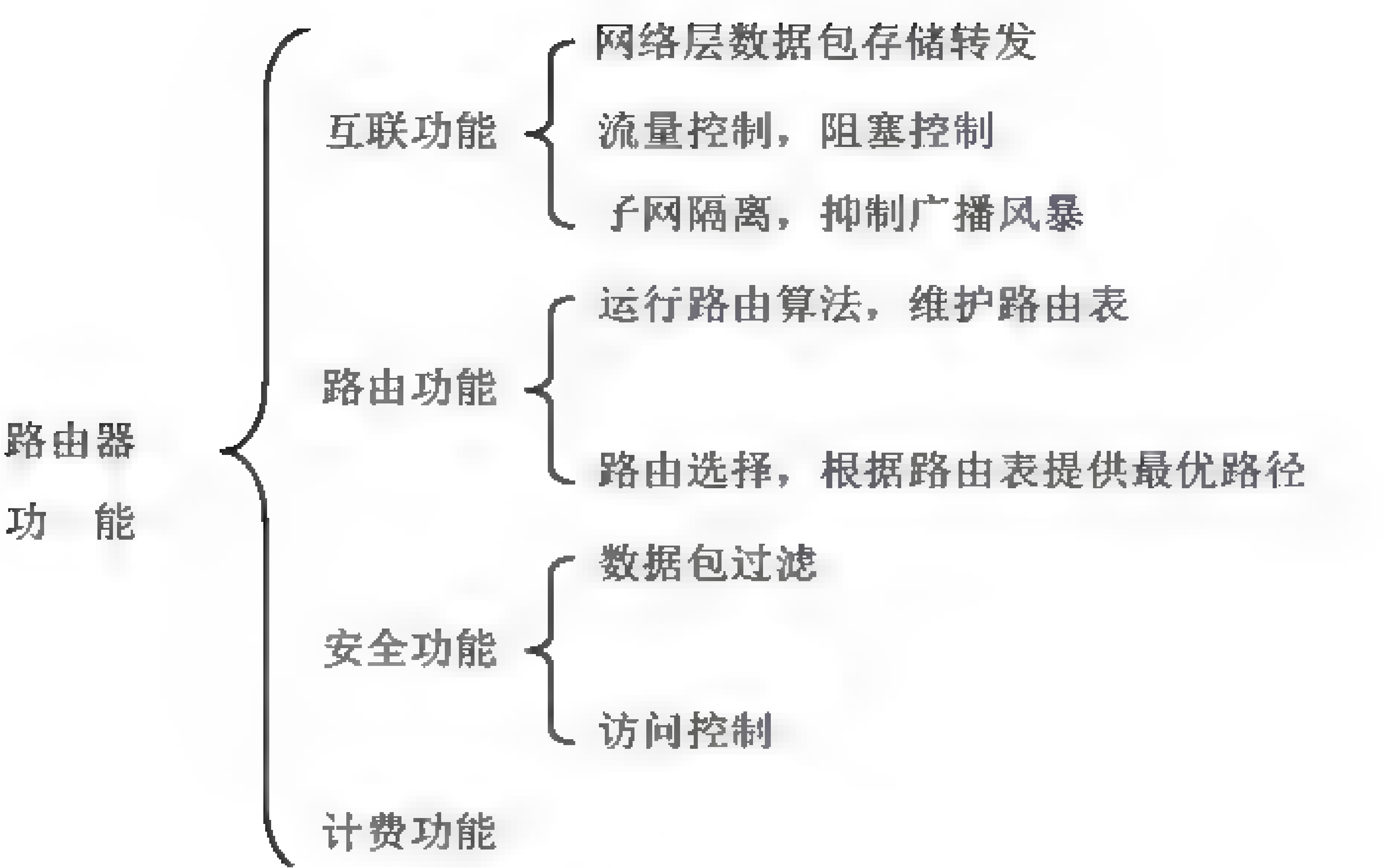


图 2-4 路由器功能

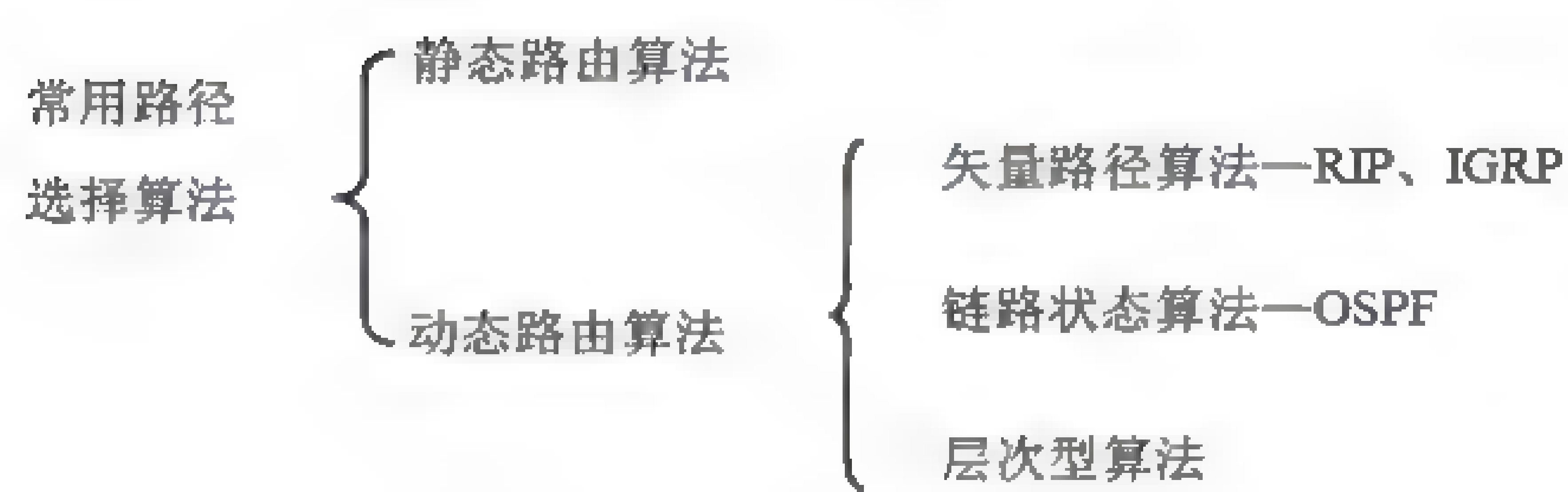


图 2-5 常用路由算法

6．网关

网关的互联是在网络层以上，具体地说，大多数的网关是在应用层实现互联。网关通常由软件实现，运行于服务器或普通计算机上，以实现不同体系结构网络之间或 LAN 与主机之间的连接。由于网关是在较高的层次上互联，所以不可能有通用网关，只可能针对某一特定应用而言，比如电子邮件网关、远程终端仿真网关等各种用途的网关。

2.1.3 网络性能

在进行网络设计时，对网络性能参数的考虑是设计工作的重点内容之一，需要考虑的网络性能参数包括响应时间、吞吐量、延迟、带宽、容量等。

1．响应时间、延迟和等待时间

响应时间、延迟和等待时间是网络的重要特性。每个特性都将对网络的性能产生影响。

响应时间是指以计算机或终端向远端资源发出请求时间为起点，以该设备接收到数据响应的时间为终点，两个时间之间的差值，这个时间直接影响到用户操作的响应效果，是评估网络用户体验的关键值。一般来说，响应时间与网络设备的处理器、电路的工作

情况有关。

响应时间根据网络结构可以分为主从结构、对等结构、两层结构、三层结构、多层结构的响应时间。

1）主从结构中的响应时间

主从结构是指网络发展早期的大型主机+终端的结构，在该结构中，主机和终端间存在着通信前置机和通信集中器。图 2-6 给出了主从结构中的响应时间组成部分。从图中可以看出，该结构的响应时间是设备上的延迟和线路延迟时间之和，是数据通过网络中的每一部分所用时间之和，每一个设备、通信连接以及处理过程的自身延迟都包含在整个响应时间之内。

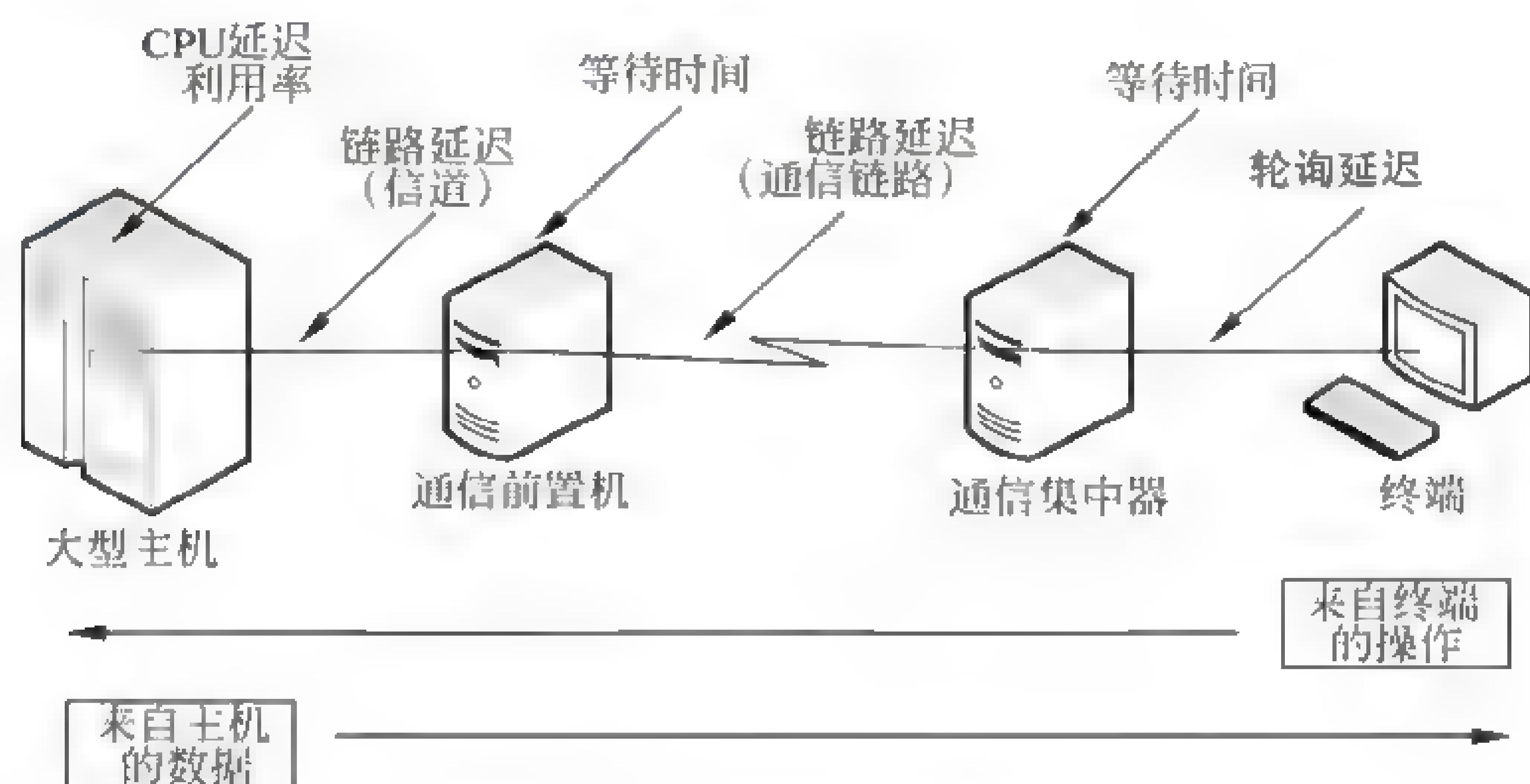


图 2-6　主从结构中的响应时间

响应时间的组成如下：

① 轮询延迟。

由于通信集中器不仅仅要处理一台终端的通信，因此存在着分时机制，由通信集中器对终端进行轮询，这是在不平衡数据通信配置结构中控制主从节点间进行通信的一种方法。如果网络终端有数据需要发送，它必须一直等到通信集中器对其进行轮询时，才能发送数据。

② 链路延迟。

链路延迟与在指定链路上传输数据的速度相关。链路的速度越快，在两点间传输数据的速度越快，则所需延迟就越短。

③ 等待时间。

等待时间是指网络设备（如通信前置机、通信集中器）在收到数据包后进行数据重组和发送所耗费的时间。

④ CPU 延迟。

CPU 延迟指的是大型主机的 CPU 处理网络请求所需要的时间，CPU 的繁忙程度、

任务的级别、任务队列长度等直接决定了请求处理的时间。

2）对等结构中的响应时间

在对等结构中，网络中的大多数主机都可以独立运行，具有运算和处理能力，所有主机的运算和处理能力相同，既可能是服务的提供者，也可能是服务的享用者。

对等结构一般存在于对等网络中，该类型网络一般采用总线结构，如图 2-7 所示。

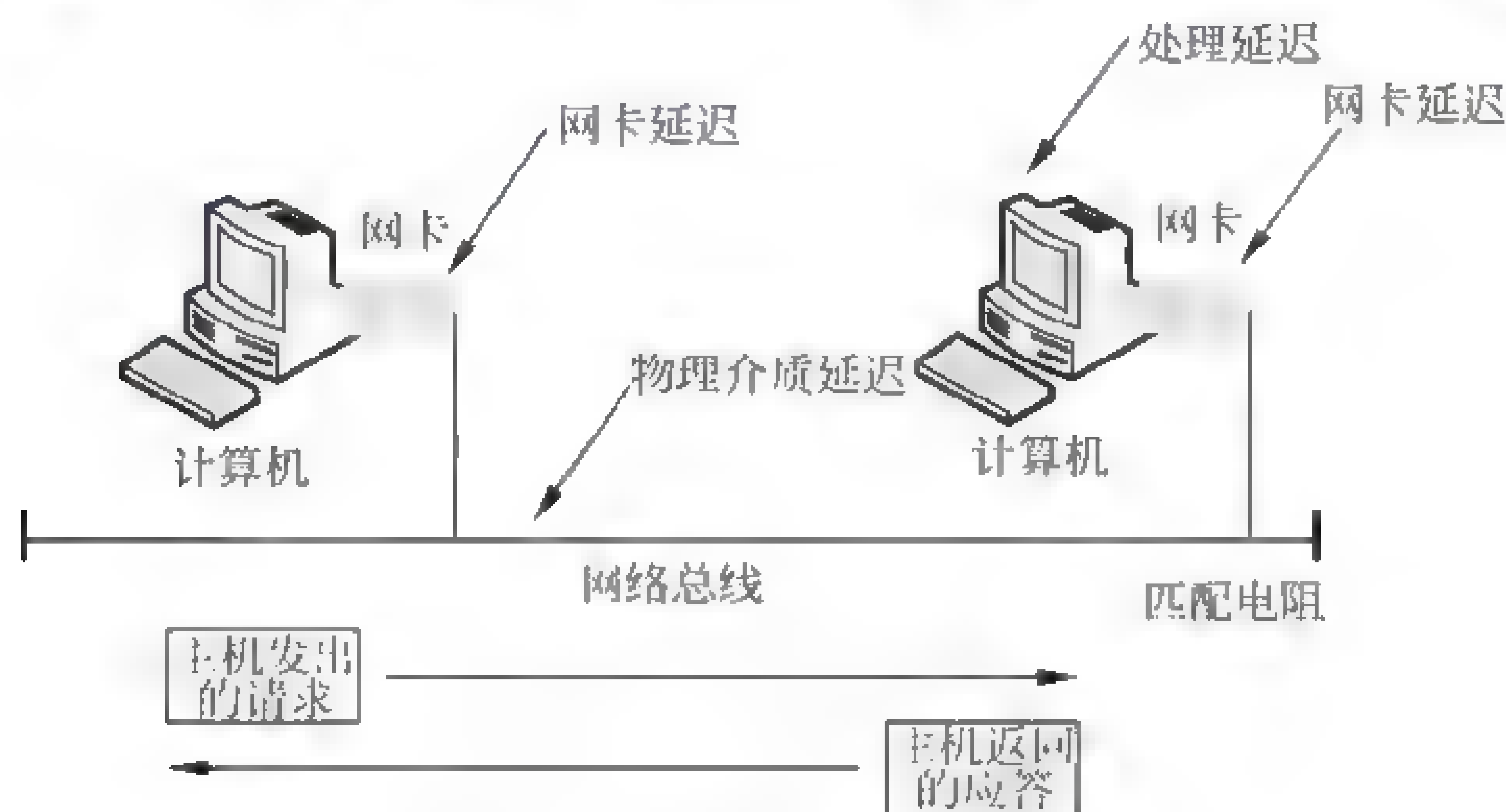


图 2-7 对等结构中的响应时间

在对等网络结构中，影响响应时间的因素主要包括：

① 网卡延迟。

网卡延迟指数据通过网卡发送到网络线路上的延迟，影响该延迟的主要因素包括介质访问冲突和吞吐率。一般来说，在共享介质中，介质上连接的主机越多，发生冲突的可能性就越大，导致数据发送开发时间推后，延迟时间加长；另外，一个相同长度的数据帧，在不同的媒体访问机制下进行数据发送时，由于吞吐量不同，需要的数据转换成为信号的时间不同，也会影响网卡延迟。在对等网络中，当主机上的一个应用程序提出一个网络连接请求时，就会产生一个延迟用于网卡处理请求并访问物理介质，进行数据发送。

② 物理介质延迟。

物理介质延迟是指信号从发送方网卡传递到接收方网卡的时间，该时间的长短取决于信号在介质上的传递速度和介质的长度。一般来说采用相同的介质和信号传递方式，则物理介质延迟时间是相同的。

③ 处理延迟。

由于接收方要对数据进行重组，并进行处理，生成响应数据，必然会产生处理延迟。处理延迟和数据包的大小、处理工作量相关。

3）两层结构中的响应时间

两层结构是网络中常见的客户机-服务器结构，在网络中由部分运算能力较强的主机

承担服务器的角色，普通主机成为客户机；在运行过程中，客户机向服务器发出请求，通过网络传递至服务器，服务器根据请求进行处理，形成应答再通过网络传递至客户机。两层结构中的响应时间指的是服务器响应客户工作站提出的请求所用的时间，如图 2-8 所示。

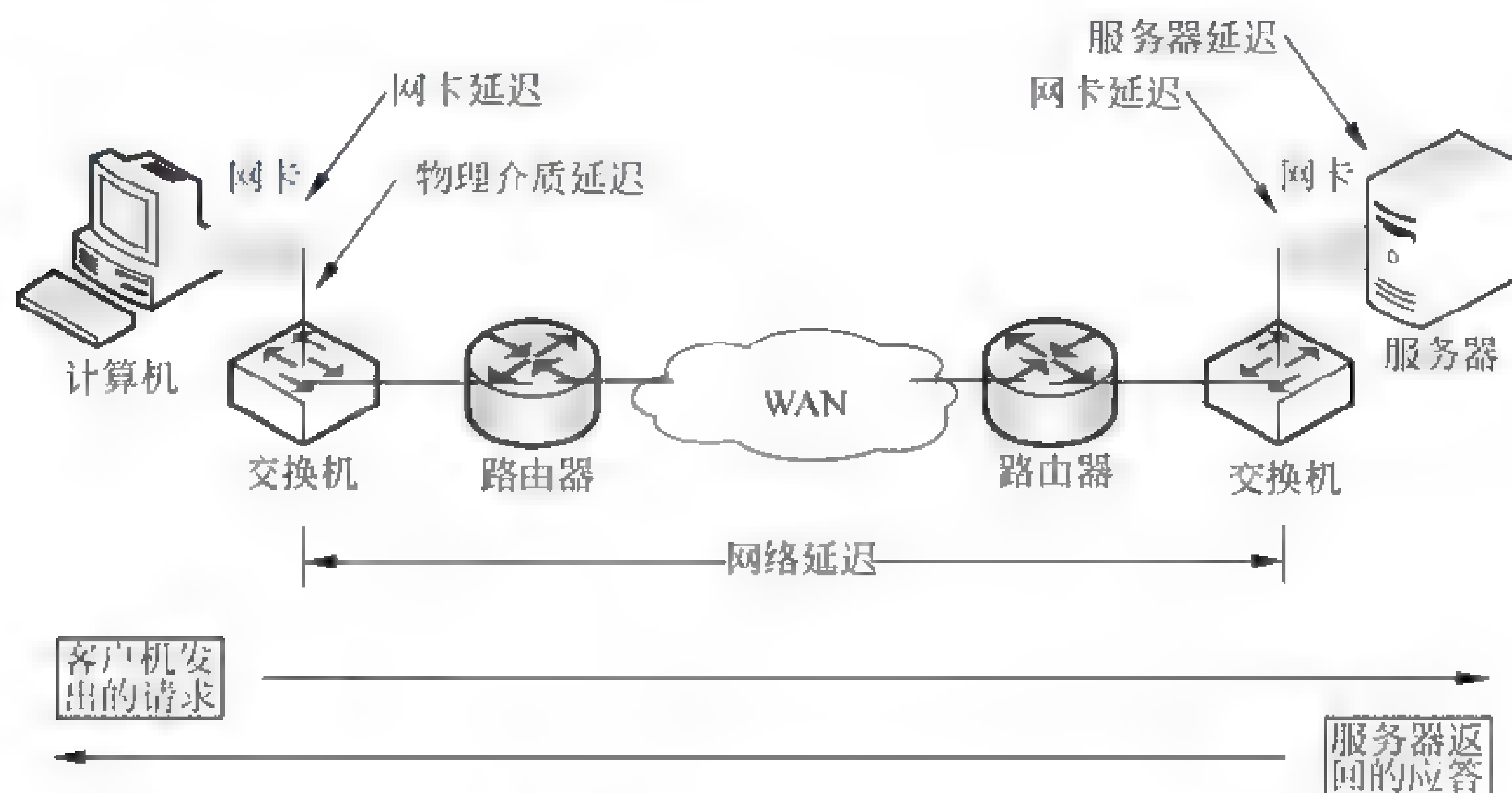


图 2-8 两层结构中的响应时间

在这种结构中，影响响应时间的因素主要有网卡延迟、物理介质延迟、服务器延迟、网络延迟等构成，其中网卡延迟、物理介质延迟与对等结构相同。

① 服务器延迟。

由于处理器的速度和服务器处理请求的平均数量不同，服务器响应时间可能会有很大的变化。影响服务器延迟的因素是队列延迟和磁盘存取延迟。

② 网络延迟。

网络延迟是两层结构中较为特殊的延迟，由于客户机、服务器可能分属于不同的局域网络，一次请求和应答的过程，可能会穿越多个局域网和广域网，请求和应答在这些网络中由于要通过多种网络设备进行存储和转发，因此网络延迟具有不确定性。一般来说，网络延迟主要来自于路由设备，由路由器间的跳数、路由设备的繁忙程度决定，由局域网交换设备产生的网络延迟要明显小于路由器。

因此，当请求 / 应答通信流通过公共广域网的时候，响应时间就会发生很大变化。例如，当使用 Internet 时，响应时间就会产生很大变化，甚至会因为超时而断开网络连接。这类网络延迟非常难以预测，而且会随时间而产生变化。

4）三层结构中的响应时间

三层结构是指由表示层、应用层、数据层形成的网络处理模式，是对两层结构的扩展，已经逐步取代两层结构成为当前网络的主流处理模式。在三层结构中，由客户机负

责与用户的交互，在客户机上不进行应用软件的部署，通常通过浏览器承担数据展现；应用层由存放应用业务逻辑的应用服务器构成，通常包括 Web 和应用程序的运行环境；数据层一般为单纯的数据库服务器。三层结构中的响应时间是指从客户机提出请求，至数据层的响应通过应用层返回客户机的时间，如图 2-9 所示。

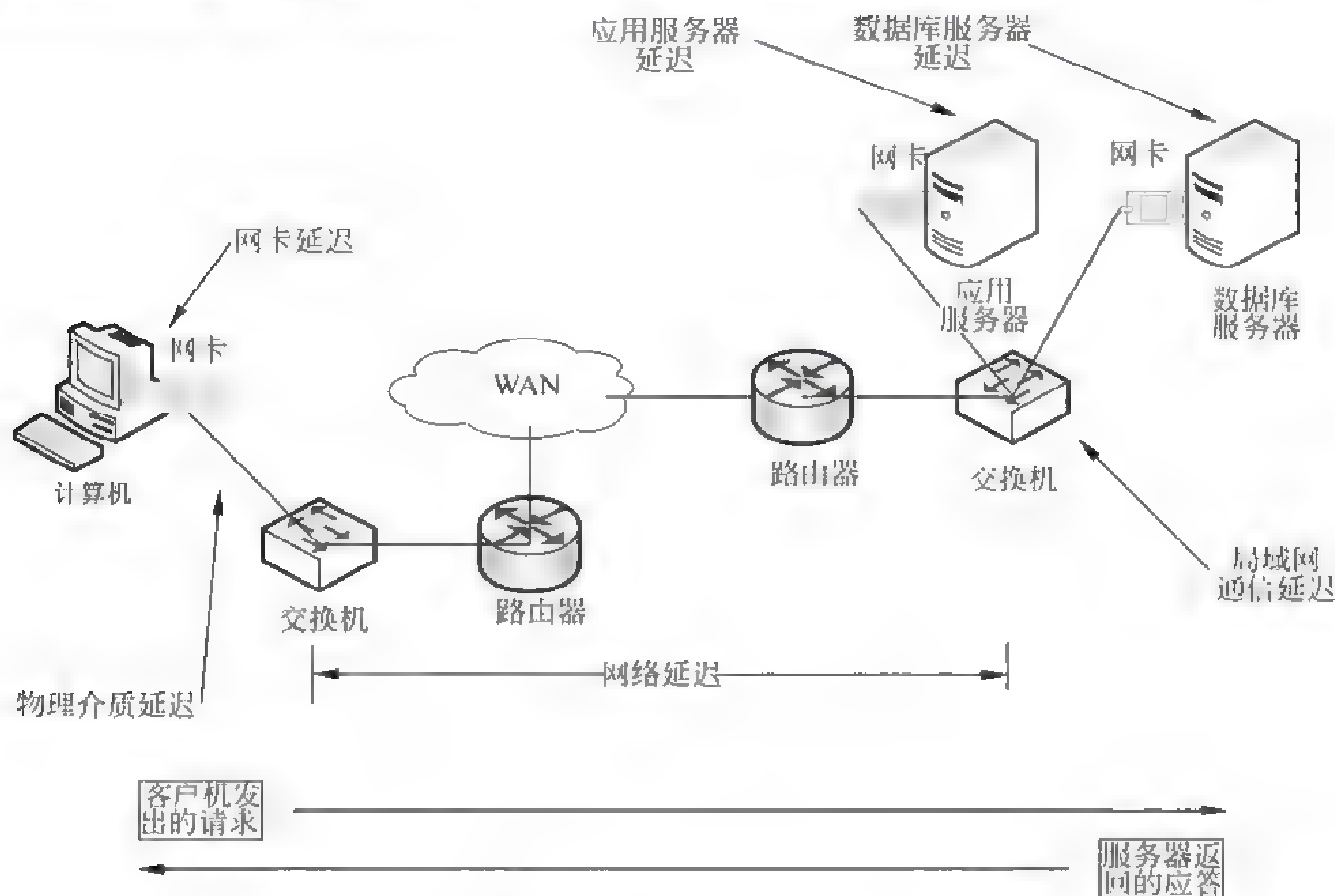


图 2-9　三层结构中的响应时间

与两层结构相比较，三层结构中影响响应时间的因素，主要增加了服务器所在局域网内部的服务器之间的延迟，包括应用服务器延迟和数据库服务器延迟，同时也增加了局域网内部通信的延迟。

① 应用服务器延迟。

由于应用服务器要对提交给 Web 服务器的请求进行处理，并形成对数据库服务器的数据请求，会产生应用服务器延迟。应用服务器的延迟主要由并发用户进程数量、CPU 繁忙程度等决定。

② 数据库服务器延迟。

数据库服务器延迟是数据库服务器针对数据检索请求进行处理，并产生数据集结果而产生的响应延迟，该延迟主要由并发用户数量、CPU 繁忙程度、磁盘 I/O 繁忙程度等因素决定。

③ 局域网内部通信延迟。

由于应用服务器和数据库服务器在一次响应过程中间，会产生一次或多次交互，这些交互多通过局域网完成，因此形成了局域网内部通信延迟，该延迟主要由局域网设备通信速率、局域网设备繁忙程度等隐私决定。

5）多层结构中的响应时间

多层结构是为了大型应用系统、数据中心的建设需要，在原有三层结构基础上，将应用服务器层次，划分为多个层次的网络处理模式。该结构中的响应时间，相对于三层结构，主要增加了多个服务器的处理延迟，以及服务器间多次交互而形成的多次局域网通信延迟。

2．利用率

利用率描述设备在使用时所能发挥的最大能力。在网络分析与设计过程中，通常考虑以下两种类型的利用率。

- CPU 利用率。
- 链路利用率。

1）CPU 利用率

CPU 利用率指的是在处理网络发出的请求和做出响应时处理器的繁忙程度。网络设备互联（如路由器）要处理的数据包越多，所耗费的 CPU 时间就越长。由于任何设备的 CPU 处理能力都是有限的，一旦出现处理能力小于待处理业务要求时，就会形成待处理业务队列，尚未获得处理机资源的进程，就会进入队列中进行等待，直至获得处理机资源而被唤醒。

路由器的 CPU 利用率将直接关系到网络的性能，当路由器的 CPU 利用率超过了某个值后，路由器不能及时处理涌入的数据包，网络的整体性能就会随之下降。在实际应用中，因为路由器必须处理转发数据以外的事务，路由器有效最大利用率一定低于 100%。例如，各个路由器之间需要交换数据来维护路由表，许多设备保存管理信息，并要求相应的网络管理命令。随着设备越来越复杂，就必须利用更多的 CPU 时间来处理这些额外的事务。

2）链路利用率

链路利用率指的是链路总带宽的有效使用百分比。在网络实际运行过程中，链路带宽等资源不一定会被全部占用，因此链路利用率是一个动态变化的值。例如，购买了一条 ISDN-PRI 线路，它有 30 条 64Kbps 的数据信道（B 信道）和 1 条 16kbps 的控制信道（D 信道），最大带宽为 2.048Mbps，如果当前只充分利用了 6 条数据信道，则这条线路的利用率就是（6×64）/（30×64+16）×100%≈19.83%，即当前的链路利用率为 19.83%。

3．网络数据传输率和吞吐量

1）网络数据传输率

在计算机网络中，数据传输率和带宽是两个不同，但又关联的概念。

带宽：指某个信号具有的频带宽度，其单位是赫兹（Hz）。一般来说，通信线路允

许通过的信号频带范围就称为线路的带宽。

数据传输率：信道上可以传输数据的最大速率，在计算机网络中，无论数字信号、模拟信号都用于传递数字数据，因此其单位为比特每秒（bps）。

如前面章节所描述，一般来说，线路的带宽越大，其允许的数据传输率就越高；同时，人们已经习惯用带宽来等同于线路上的数据传输率；实际上，两者之间有一定的联系，但并不是相等的关系。表 2-2 中列举了常见数据传输技术的数据传输率。

表 2-2 常见技术的数据传输率

技术类型	数据传输率	物理媒体	应用环境
拨号线路	14.4～56Kbps	双绞线	本地和远程低速访问，主要用于偏远地区的网络访问
租用线路	56Kbps	双绞线	小型商业低速访问
综合业务数字网（ISDN）	128Kbps	双绞线	小型、中型商业应用，用于电话和网络公用
卫星（直接用 PC）	400Kbps～2Mbps	无线电波	移动条件下、偏远地区的低速网络访问
帧中继	56Kbps～1.544Mbps	双绞线	小型或中等商业应用
T1	1.544Mbps	双绞线、光纤	中等商业应用、Internet 访问、端到端网络连通
E1	2.048Mbps	双绞线、光纤	中等商业应用、Internet 访问、端到端网络连通
ADSL	1.544～8Mbps	双绞线	主要用于家庭、小型商业 Internet 访问应用
电缆调制解调器	512Kbps～52Mbps	同轴电缆	主要用于家庭、中小型商业应用，是实现三线合一的主要技术
以太网	10Mbps	同轴电缆或双绞线	局域网
令牌环网	4Mbps 或 16Mbps	双绞线	局域网
E3	34.368Mbps	双绞线或光纤	16 个 E1 信号
T3	45Mbps	同轴电缆	连接 ISP 到 Internet 基础结构、大型商业应用
0C-l	51.84Mbps	同轴电缆	骨干网、校园网连接 Internet ISP 到骨干网
快速以太网	100Mbps	双绞线、光纤、同轴电缆	高速局域网
光纤分布式数据接口（FDDI）	100Mbps	光纤	局域网骨干
铜线分布式数据接口（CDDI）	100Mbps	双绞线	主机连通

续表

技 术 类 型	数据传输率	物 理 媒 体	应 用 环 境
OC-3	155.52Mbps	光纤	大型公司骨干网
千兆位以太网	1Gbps	光纤铜线（受限）	高速局域网的连通
OC-24	1.244Gbps	光纤	Internet 骨干网、高速的公司骨干网
OC-48	2.488Gbps	光纤	Internet 骨干网

为能够正常地发挥作用，不同类型的应用需要不同的网络带宽。一些典型应用的网络带宽如下。

- PC 通信：14.4～56Kbps。
- 数字音频：1～2Mbps。
- 压缩视频：2～10Mbps。
- 文档备份：10～100Mbps。
- 非压缩视频：1～2Gbps。

2）吞吐量

吞吐量是指在网络用户之间有效地传输数据的能力。如果说数据传输率给出了网络所能传输的比特数，那么吞吐量就是它真正有效的数据传输率。吞吐量常用来评估整个网络的性能。对吞吐量进行度量的一种有效方法是信息比特吞吐率（TRIB），有效吞吐量与响应时间直接相关，有效吞吐量越高，响应时间就越短。有效吞吐量和吞吐量通常是等同的，只有在特别需要时才加以区分。一般以数据包每秒（PPS）、字符每秒（CPS）、事务处理数每秒（TPS）或事务处理数每小时（TPH）作为吞吐量的单位。

影响吞吐量的因素如下：

- 协议效率，不同的协议传输数据的效率不同。
- 服务器/工作站 CPU 类型。
- 网卡（NIC）类型。
- 局域网（LAN）/链路容量。
- 响应时间。

事务处理数每秒和事务处理数每小时是最常用的度量吞吐量的单位，例如，7200TPH 或者 2TPS。仅知道 TPH 还不足以衡量整个网络的性能，还必须知道 TPH 的平均大小和一天中什么时间发生的 TPH。

4．可用性、可靠性和可恢复性

1）可用性

可用性是指网络或网络设备（如主机或服务器）可用于执行预期任务时间所占总量的百分比。可用性百分值越高，就意味着设备或系统出现故障的可能性越小，提供的正常服务时间越多。例如，一个可提供每天 24 小时、每周 7 天服务的网络，如果网络在

168 小时（一周）之内运行了 160 小时，出现了 4 个小时的故障排除，则该网络的可用性为 160/（7×24）×100%=95.23%。

可用性通常表示平均可运行时间，95%可用性意味着 1.2 小时 / 天的停机时间，而 99.99%的可用性则表示 8.7 秒 / 天的停机时间。

对于大多数设备来说，可用性百分之百是不可能的，但是对于一个网络或者系统来说，则可以做到可用性百分之百；为了保证一个系统能够不间断地提供服务，必须采用特殊的设计，例如设备冗余、负载均衡等，避免单个设备的故障对系统服务产生影响，这种设计也被称为无单点故障设计。

2）可靠性

可靠性是网络设备或计算机持续执行预定功能的可能性。可靠性经常用平均故障间隔时间（MTBF）来度量。这种可靠性度量也适用于硬件设备和整个系统。它表示了系统或部件发生故障的频率。例如，一个 MTBF 如果为 5800 小时，则意味着大约每 8 个月可能发生一次故障。

在网络设计中，可靠性设计主要考虑下述问题：

- 一个特殊设备在网络中发生故障的可能性有多大?
- 设备的故障是否会导致网络的崩溃?
- 网络的故障将会对企业的生产力产生什么样的影响?

可靠性与可用性紧密相关。它们都是企业计算环境设计的目标。可用性可用来度量可靠性，可用性越高，可靠性越好。

3）可恢复性

可恢复性是指网络从故障中恢复的难易程度和时间。可恢复性即指平均修复时间（MTTR）。平均修复时间用来估算当故障发生时，需要花多长时间来修复网络设备或系统。影响 MTTR 的因素有以下一些：

- 维护人员的专业知识。
- 设备的可用性。
- 维护合同协议。
- 发生时间。
- 设备的使用年限。
- 故障设备的复杂程度。

在设备或系统方面，不同的设备需要不同级别的可恢复性。例如，数据中心的核心交换设备一旦出现故障，其修复难度将远远大于楼栋交换机的修复难度。

需要说明的是，可恢复性指标主要是通过平均修复时间来说明修复工作的难易程度的，这种评估方法是从用户角度来衡量网络的关键指标，其核心思想是相同的故障，在管理水平不同的网络中，其修复时间是不同的，用户所承受的网络损失也不同。在实际的网络维护工作中，管理人员可以通过良好的管理制度，例如定期设备巡检、设备配置

备份、充足的冗余设备备份等，来减少故障发生时的修复时间，从而达到提高整个网络可恢复性的目的。

5．冗余度、适应性、可伸缩性

1）冗余度

冗余设备是指为避免由于单台设备故障而导致网络停止服务而增加的网络设备。冗余线路是指为了防止线路或链路失效，导致网络不连通而增加的多余线路。冗余度是另一个在网络设备和系统设计与实施中需要考虑的因素，主要通过在网络设计中增加冗余设备、冗余线路等方式，来避免设备或线路失效对网络产生影响。随着计算机网络技术的发展，冗余度也不再仅局限于设备和线路层次，更多的冗余度开始体现到网络设备的模块、部件层次，今天在网络设计中，为关键网络设备添加冗余处理引擎、冗余电源等方式，已经成为常见的技术手段。

（1）冗余线路。

冗余线路是指在局域网或广域网的设计中，针对关键的通信线路，通过提供多条线路，避免单条线路失效而导致网络失效。冗余线路的使用方式，有人工切换方式、热备方式、负载均衡方式，如图 2-10 所示。

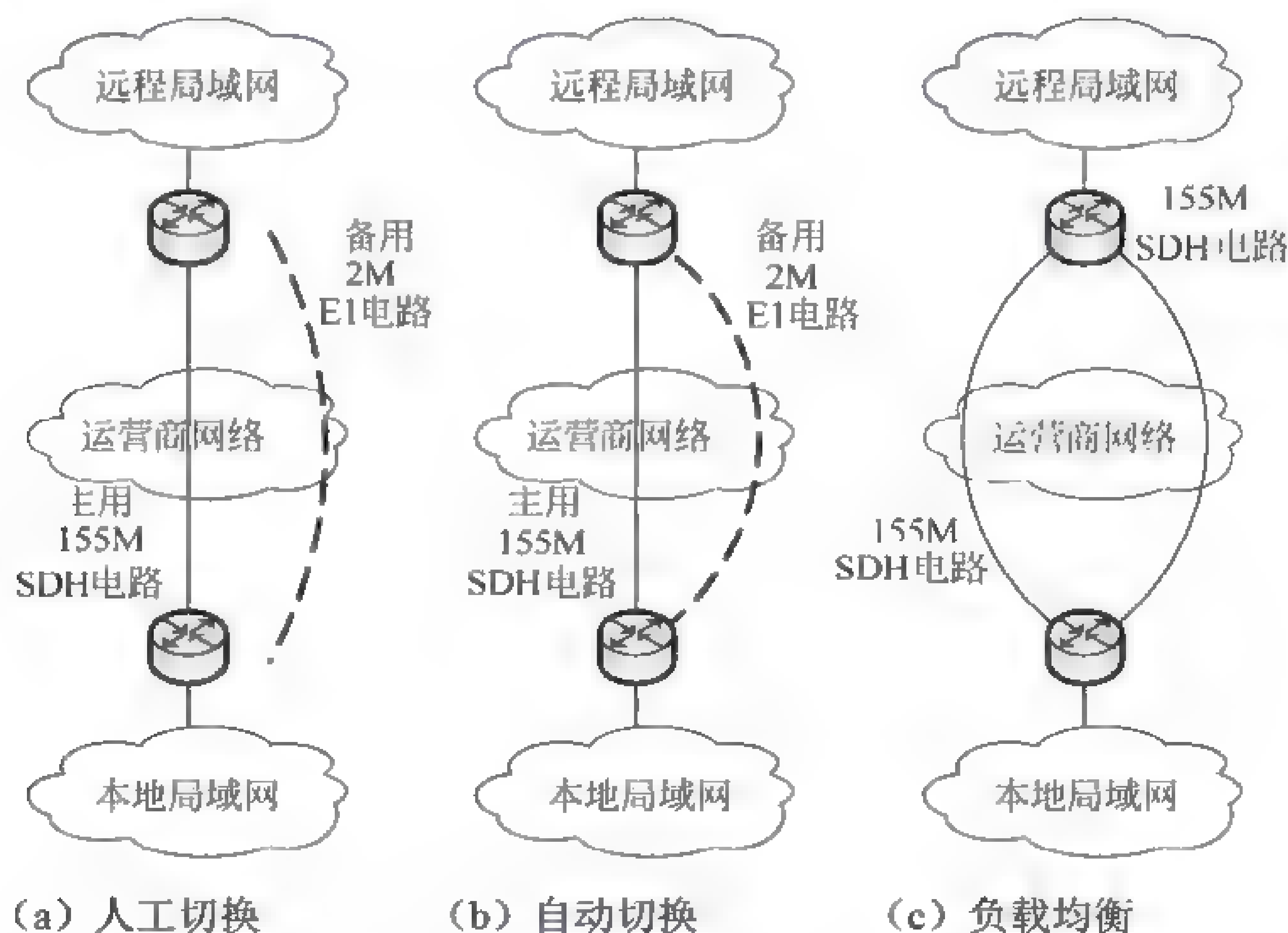


图 2-10　冗余线路建设方式

在图 2-10 所示的网络连接中，远程局域网络和本地局域网络之间通过运营商提供的线路和路由器实现互联。人工切换方式中，网络管理人员申请了备用线路，在主用线路出现故障时，由网络管理人员将备用线路连接至路由器，并启用备用线路的配置，使得备用线路生效；在自动切换方式中，主用线路和备用线路都连接至路由设备，正常工作

状态下，主用线路生效，备用线路处于热备状态，由路由器自动监测主用线路，一旦主用线路出现故障，则路由器自动启用备用线路，并切换至备用线路运行；在负载均衡方式下，网络管理员申请两条同样或相近带宽的线路，由路由器的特定路由算法保证两条链路都处于运行状态，两个网络中的流量同时在两条线路上进行传递。

（2）冗余设备。

在计算机网络中，对于关键设备，提供两个以上，并处于热备或者负载均衡状态，以避免由于设备失效而导致的网络整体失效，如图 2-11 所示。

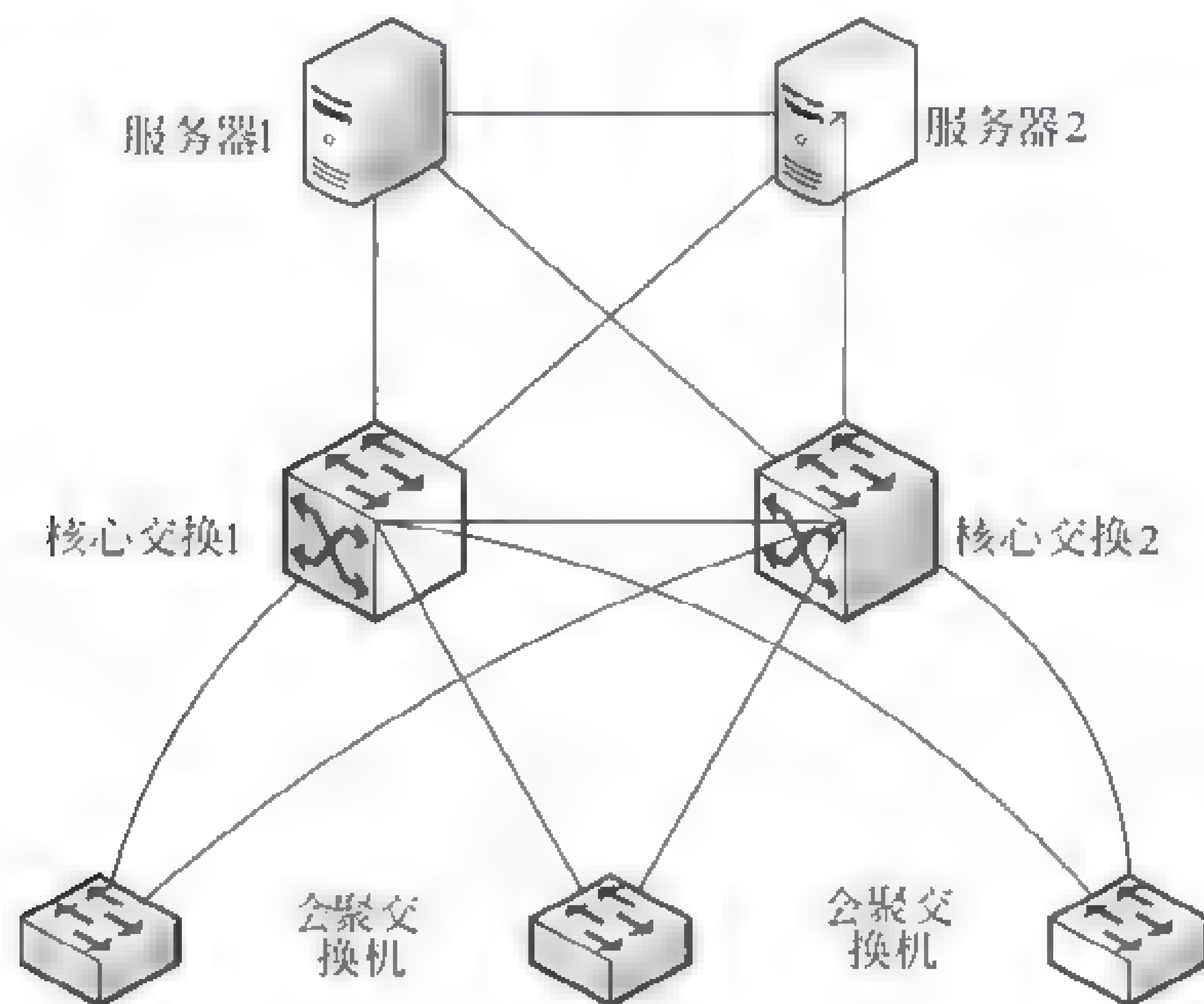


图 2-11　冗余线路建设方式

在图 2-11 的网络中，为了避免核心交换机和服务器出现故障，各添加了一台服务器和核心交换机；两台核心交换机之间可以工作在热备状态，也可以工作在负载均衡状态，不同状态使用的协议不同；服务器之间根据应用的需要，例如如果是 Web 服务器，多工作在负载均衡状态，如果是应用服务器或者是数据库服务器，多工作在热备状态；在这个网络中，核心设备出现故障，服务会自动切换到冗余的设备上。

（3）冗余模块。

典型的冗余模块较多，例如核心多层交换机上的冗余路由引擎，网络设备和服务器设备上的冗余电源与风扇，服务期设备上的镜像内存，存储设备的热备硬盘等。

在重要的网络设计中，网络冗余度是必须考虑的内容，可根据用户的保护需求以及投资概算决定冗余度的不同层次。

2）适应性

适应性是指在用户改变应用要求时网络的应变能力。优秀的网络设计应当能适应新技术和新变化的要求。例如，使用笔记本计算机的移动用户对能访问企业局域网来实现

E-mail 和文件传输服务的需求正是对网络适应性的检验。

灵活的网络设计还能适应不断变化的通信模式和服务质量（QoS）的要求。例如，某些用户要求选用的网络技术能够支持提供恒定速率的服务。

此外，以多快的速度适应出现的问题和进行升级也是适应性的另一方面。例如，交换机能以多快的速度适应另一个交换机的故障，或适应树状拓扑结构发生的变化；路由器能以多快的速度适应加入拓扑结构的新网络等。

3）可伸缩性

可伸缩性是指网络技术或设备随着用户需求的增长而扩充的能力。对于许多企业网设计而言，可伸缩性是最基本的目标。有些企业常以很快的速度增加客户数量、应用种类以及与外部的连接。因此在网络分析和设计时就应充分考虑网络扩充问题。

6．效率与费用

1）网络效率

网络效率指的是用户传输数据流量与网络线路带宽之间的比例。不同的网络传输技术，其网络效率是不同的。网络划分成若干个层次，因此每个层次间都存在上层用户数据与下层数据通道的效率问题，但是在大多数情况下，网络设计时主要考虑数据链路层的网络效率。

网络效率的计算公式为效率=（帧长–帧头和帧尾）/（帧长）×100%，额外开销指不能用于传输用户数据的带宽比例，额外开销=（1–效率）；在 ATM 网络中，由于信元长度固定为 53 个字节，信元头部固定为 5 个字节，因此，ATM 的网络效率为（53–5）/53×100%=90.5%，额外开销=1–90.5%=9.5%；在传统以太网络中，由于以太网的帧头大小固定，而用户数据不固定，但有最小帧长和最大帧长，因此以太网的最小网络效率为（64–18）/64×100%=71.9%，最大额外开销为 28.1%，最大网络效率为（1518–18）/1518×100%=98.8%，最小额外开销为 0.02%，实际应用中，要根据以太网的平均帧长来计算平均网络效率。

2）费用

费用是建设网络时必须考虑的内容，网络建设费用包括很多内容，例如设备购置费用、安装调试费用、线路租赁费用、设备运维费用，一般情况下，网络设计人员会将网络建设费用划分为两种，一种是一次性投入费用，另外一种是周期性发生费用。费用是网络建设中对网络建设制约比较大的因素，应根据用户在一次性费用和周期性费用方面的投入来决定如何设计网络。

2.1.4　网络设计文档

1．文档的作用

文档是网络设计工作中的重点环节，覆盖了需求规范、通信规范、逻辑设计、物理设计、网络实施、运营维护等各个阶段，通过对网络分析、设计实现等阶段的细节进行

描述，说明开发一个网络的步骤。

文档的编制在网络项目开发工作中占有突出的地位。高效率、高质量地开发、分发、管理和维护文档对于转让、变更、修正、扩充和使用文档，以及充分发挥网络产品的效益都有着重要的意义。

网络开发过程中，网络开发人员需要制定一些工作计划或工作报告，这些计划和报告要提供给管理人员，并得到必要的支持。管理人员则可通过这些文档了解网络开发项目的安排、进度、资源使用和成果等。

文档的重要性总结如下：

- 提高网络设计过程中的可见度。把设计过程中发生的事件以某种可阅读的形式记录在文档中，管理人员可以把这些记载下来的材料作为检查项目设计进度和设计质量的依据，实现对网络设计工作的管理。
- 提高设计效率。项目文档的编制使得开发人员对各个阶段的工作都进行周密思考、全盘权衡，从而减少返工。并且可在开发早期发现错误和不一致性。
- 作为设计人员在一定阶段的工作成果和结束标识。
- 记录设计过程中的有关信息，便于协调以后的系统设计、使用和维护。
- 提供有关系统的运行、维护和培训的信息，便于管理人员、开发人员、操作人员、用户之间的协作、交流和了解，使网络设计活动更加科学、更加有效。
- 便于潜在用户了解系统的功能、性能等各项指标，为他们选购或制订符合自己需要的系统提供依据。

从某种意义上讲，文档是网络分析与设计规范的体现和指南。按规范要求生成一套文档的过程，就是按照网络分析与设计规范完成了一个网络项目分析与设计的过程。所以，在进行网络设计的过程中，应当充分注意文档的编制和管理。

从形式上看，文档大致可以分为两类：一类是网络设计过程中填写的各种图表，可称为工作表格；另一类是应编制的技术资料或技术管理资料，可称为文档或文件。

文档的编制可以用自然语言，特别设计的形式语言，或是介于两者之间的半形式语言（结构化语言）以及各类图表和表格来表示。文档可以书写，也可以在计算机支持的系统中产生，但它必须是可以阅读的。

在网络分析与设计过程中，产生的文档有需求分析说明书、通信规范说明书、逻辑网络设计说明书和物理网络设计说明书，这些文档作为网络设计人员前一阶段工作成果的体现和后一阶段工作的依据。

2．文档的质量

文档的编制必须保证质量，以发挥文档的指导作用，有助于管理人员监督和管理系统开发，有助于用户了解系统开发的工作，有助于维护人员进行有效的修改和扩充。高质量的文档应当体现在以下方面。

（1）针对性。

文档编制之前应分清读者对象，根据不同类型、不同层次的读者决定文档的具体内容。

（2）精确性。

文档的行文应当十分确切，不能出现多义性的表述。

（3）清晰性。

文档编写应力求简明，如有可能，配以适当的图表，使文档简洁明了。

（4）完整性。

任何一个文档都应当是完整、独立、自成体系的。

（5）灵活性。

各种不同的项目系统，其规模和复杂程度有着许多实际差别，需仔细具体地分析安排其内容，一般应注意以下问题。

① 应根据具体的项目开发，决定编制的文档种类。

② 当所开发的项目非常大时，一个文档可以分为若干分册。

③ 应根据任务的规模、复杂性、项目负责人对系统开发过程及运行环境所需详细程度的判断，确定文档的详细程度。

④ 可对各条款进行进一步细分，与之相反，也可以根据情况压缩合并。

⑤ 对文档的表现形式没有规定或限制，可以使用自然语言，也可以使用形式化语言。

⑥ 当通用文档类型不能满足项目开发特殊要求时，可以建立一些特殊的文档种类。

3. 文档的管理和维护

在整个网络生存期中，各种文档需作为半成品或是最终成品不断地生成、修改或补充。为了最终得到高质量的产品，达到所提出的质量要求，必须加强对文档的管理。对文档进行管理时应注意以下几方面：

（1）网络开发小组应设一位文档保管人员，负责集中保管项目已有文档的两套主文本。两套文本内容完全一致，其中的一套可按一定手续，办理借阅。

（2）网络开发小组的成员可根据工作需要自己保存一些个人文档。这些一般都应是主文本的复件，并注意和主文本保持一致，在做必要的修改时，也应先修改主文本。

（3）开发人员个人只保存主文本中与其工作相关的部分文档。

（4）新文档取代了旧文档后，管理人员应及时注销旧文档。在文档内容有变动时，管理人员应随时修订主文本，使其反映更新了的内容。

（5）在软件开发过程中，可能发现需要修改已完成的文档，特别是针对规模较大的项目，主文本的修改必须特别谨慎。修改以前要充分估计修改可能带来的影响，并且要按照提议、评议、审核、批准、实施等步骤加以严格的控制。

（6）项目开发结束时，文档管理人员应回收开发人员的个人文档，发现个人文档与主文本有差别时，应立即着手解决。

2.2 网络分析与设计过程

2.2.1 网络规范

当设计人员依据用户的特定网络需求进行分析和设计时，必须遵循一定的处理规范。在网络规划过程中，优秀的、正规的设计过程将避免设计者工作过程中产生的失误和错误，同时产生合理有效的设计方案，并保证最终根据网络设计形成满足用户需求的网络工作环境。

以下是由于设计工作不遵循规范而产生的常见问题，这些问题将会导致用户的网络应用满意度降低。

1. 实施结果偏离网络需求

网络设计规范是大量工作经验的积累成果，覆盖了网络分析与设计过程中的方方面面，不采用设计规范，包括文档格式、调查手段等，就会使得网络需求产生缺失，同时如果没有及时与用户进行交流和取得一致意见，设计者将不会清楚实际需求，最后，也不可能得到一个满足需求的网络。

2. 需求变更

在网络的分析、设计以及实施过程中，用户的需求产生变更是正常的，因此在整个过程中，必须有一套较为完整的需求变更控制机制，设计人员必须依据变更控制规范，不断修正合理的需求变化，对不合理的用户需求进行劝导和说服。需求变更控制的重点不是限制用户的需求发生变更，而是协助用户明确自身的需求，通过双方认同的确认方式，例如现场讨论、研讨会、需求文档签字确认等手段，使双方明确需求，并明确需求可以发生变动的领域和趋势，从而保证分析和设计工作的延续性，避免颠覆性变更。

3. 延误工期或超支

进度控制和成本控制是网络分析和设计工作的重点，依据网络规范进行分析和设计工作，可以避免工期设计的不合理，也可以严格控制网络建设的成本，同时通过积累的大量文档模板，可以避免由于缺失网络建设工作中的环节和事项，而导致的工期延误和超支。

4. 网络实施和设计不一致

网络建设工作中，主要是购置相应的产品，进行网络的构建，所有的设计工作都必须依据特定的网络产品，这些网络产品必须是可以购置到的，并且相互之间可以实现互连。如果不遵循网络规范，很容易形成设计与实施不一致，常见的不一致体现在以下方面。

- 无法购置到满足设计要求的产品。
- 购置的网络产品由于其产品的特性，无法依据设计的连接方式实现互连。

- 由于设计中采用了非主流设计方法，使得线路运营商无法提供满足设计要求的互连线路。
- 在实施过程中，发现现有设计方案缺乏扩展性，而不得不重新设计。

对于大型复杂的网络工程项目，需要规范化、文档高度精确化。遵循规范进行处理并不会加大项目的工作量，反而使设计者的工作简单、高效和满足需求。

2.2.2　网络生命周期

一个网络系统从构思开始，到最后被淘汰的过程被称为网络的生命周期；一般来说网络的生命周期至少包括网络系统的构思计划、分析设计、实时运行和维护的过程；对于大多数网络系统来说，由于应用的不断发展，这些网络系统需要不断重复设计、实施、维护的过程。

因此，网络系统的生命周期和软件工程中的软件生命周期非常类似，首先是一个循环迭代的过程，每次循环迭代的动力都来自于网络应用需求的变更；其次每次循环过程中，都存在需求分析、规划设计、实施调试和运营维护等阶段。有些网络仅仅经过一个周期就被淘汰，而有些网络在存活过程中经过多次循环周期，一般来说，网络规模越大、投资越多，则其可能经历的循环周期也越多。

1．网络生命周期的迭代模型

网络生命周期的迭代模型的核心思想是网络应用驱动理论和成本评价机制，当网络系统无法满足用户的需求时，就必须进入到下一个迭代周期，经过迭代周期后，网络系统将能够满足用户的网络需求；成本评价机制决定是否结束网络系统的生命周期，当对已有投资的再利用成本小于新建系统的成本时，网络系统可以进入下一次迭代周期，而再利用成本大于新建成本时，就必须舍弃迭代，终结当前网络系统，新建网络系统。网络生命周期的迭代模型如图 2-12 所示。

2．迭代周期的构成

每一个迭代周期，都是一个网络重构的过程，不同的网络设计方法中，对迭代周期的划分方式是不同的；这些划分方式侧重点不同，拥有不同的网络文档模板，但是实施后的效果都是满足了用户的网络需求；目前没有哪个迭代周期可以完美描述所有项目的开发构成，但是常见的构成方式主要有三种。

1）四阶段周期

四阶段周期的特点是，能够快速适应新的需求，强调网络建设周期中的宏观管理，灵活性较强。

如图 2-13 所示，4 个阶段分别为构思与规划阶段、分析与设计阶段、实施与构建阶段和运行与维护阶段，这 4 个阶段之间有一定的重叠，保证了两个阶段之间的交接工作，同时也赋予了网络工程设计的灵活性。

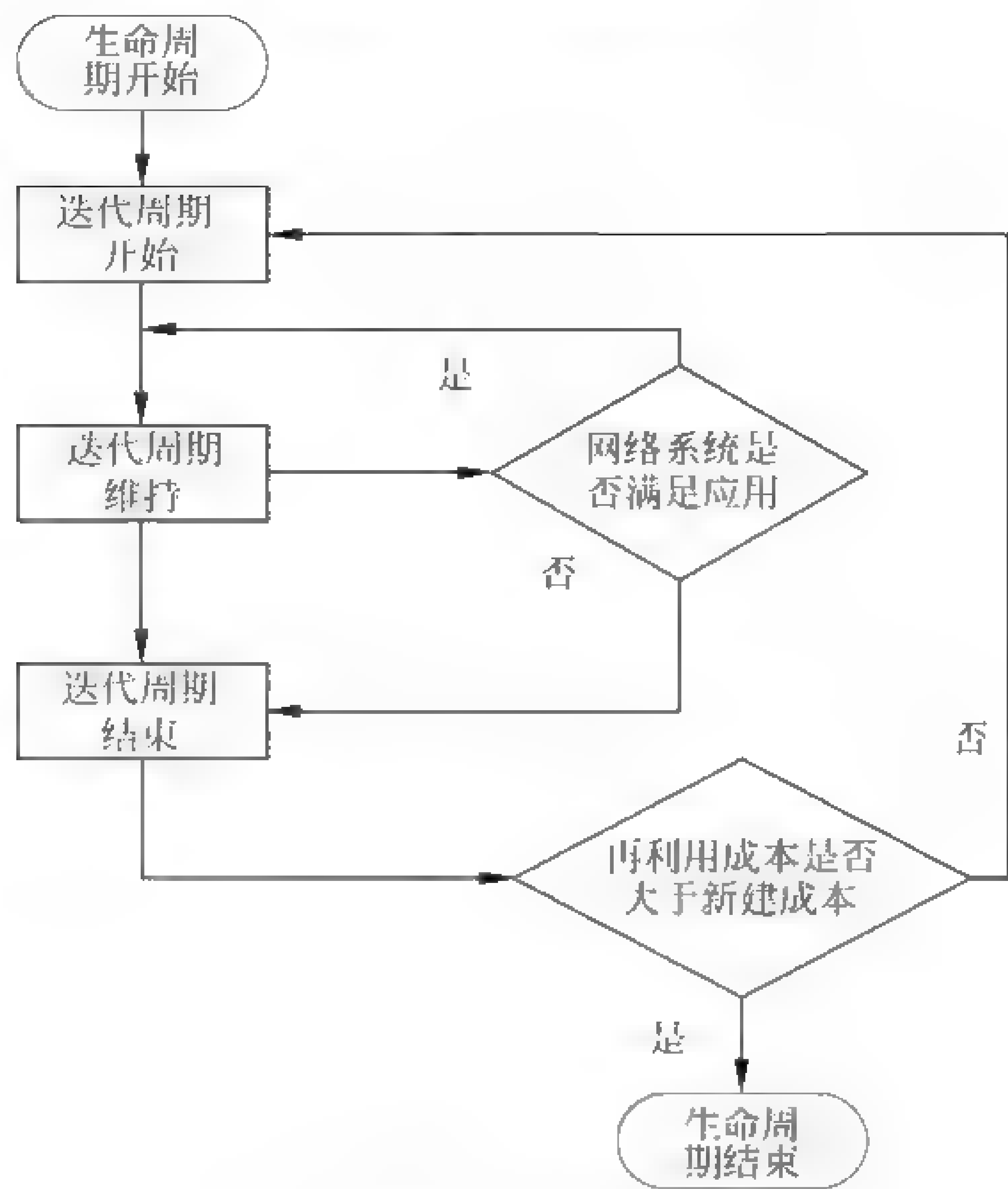


图 2-12 网络生命周期的迭代模型

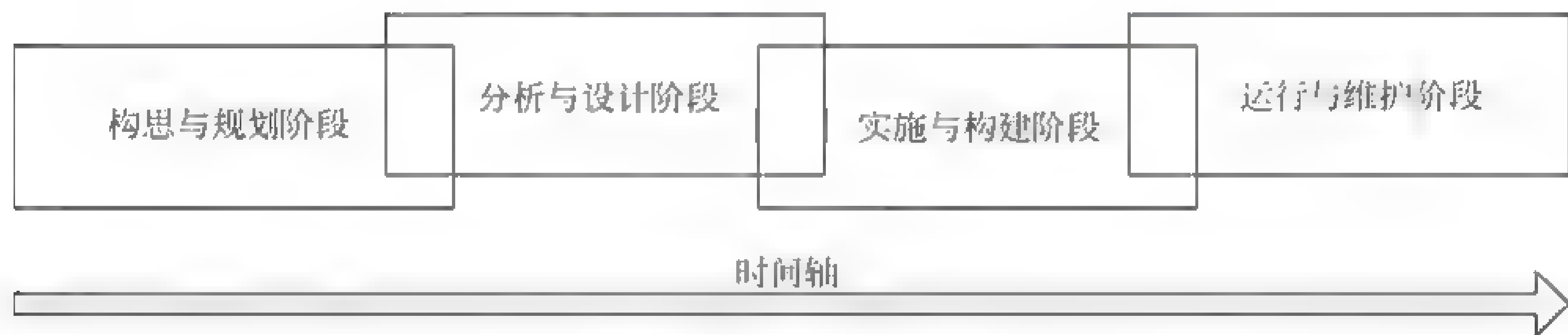


图 2-13 四阶段周期

构思与规划阶段的主要工作是明确网络设计或改造的需求，同时对新网络的建设目标进行明确；分析与设计阶段的工作在于根据网络的需求进行设计，并形成特定的设计方案；实施与构建阶段的工作在于根据设计方案进行设备购置、安装、调试，形成可试用的网络环境；运行维护阶段提供网络服务，并实施网络管理。

四阶段周期的长处在于工作成本较低、灵活性高，适用于网络规模较小、需求较为明确、网络结构简单的网络工程。

2）五阶段周期

五阶段周期是较为常见的迭代周期划分方式，将一次迭代划分为 5 个阶段。

- 需求规范。

- 通信规范。
- 逻辑网络设计。
- 物理网络设计。
- 实施阶段。

在 5 个阶段中，由于每个阶段都是一个工作环节，每个环节完毕后才能进入到下一个环节，类似于软件工程中的“瀑布模型”，形成了特定的工作流程，如图 2-14 所示。

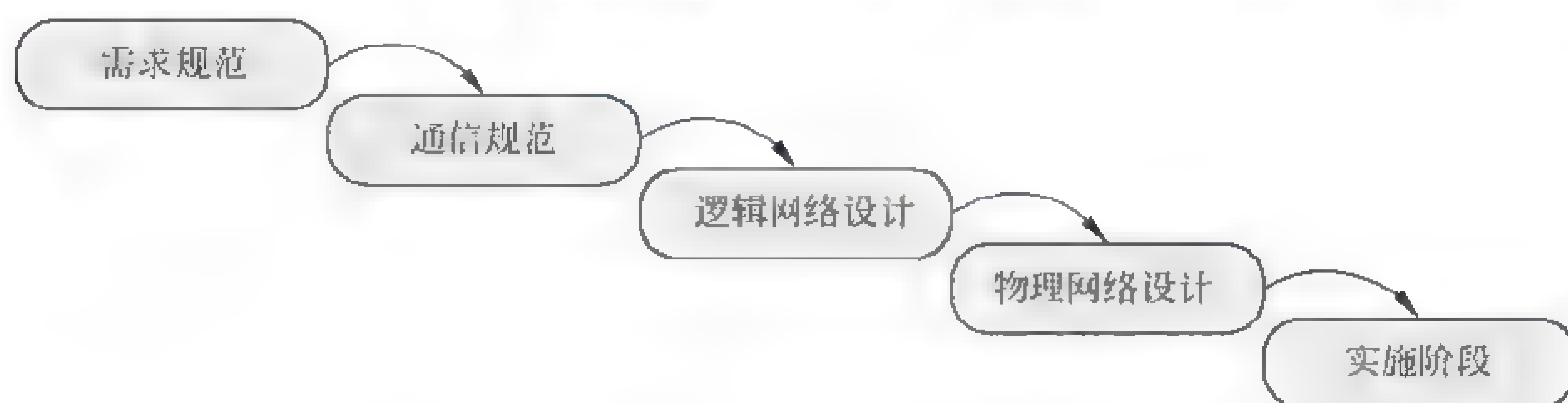


图 2-14　五阶段周期

按照这种流程构建网络，在下一个阶段开始之前，前面的每个阶段的工作必须已经完成。一般情况下，不允许返回到前面的阶段，如果出现前一阶段的工作没有完成就开始进入下一个阶段，则会对后续的工作造成较大的影响，甚至产生工期拖后和成本超支。

五阶段周期的主要优势在于所有的计划在较早的阶段完成，该系统的所有负责人对系统的具体情况以及工作进度都非常清楚，更容易协调工作。

五阶段周期的缺点是比较死板，不灵活。因为往往在项目完成之前，用户的需求经常会发生变化，这使得已开发的部分需要经常修改，从而影响工作的进程，所以基于这种流程完成网络设计时，用户的需求确认工作非常重要。

五阶段周期由于存在较为严格的需求和通信分析规范，并且在设计过程中充分考虑了网络的逻辑特性和物理特性，因此较为严谨，适用于网络规模较大，需求较为明确，在一次迭代过程中需求变更较小的网络工程。

五阶段周期将在后续章节中进行详细介绍。

3）六阶段周期

六阶段周期是对五阶段周期的补充，是对其缺乏灵活性的改进，通过在实施阶段前后增加相应的测试和优化过程，提高网络建设工程中对需求变更的适应性。

6 个阶段分别由需求分析、逻辑设计、物理设计、设计优化、实施及测试、监测及性能优化组成，如图 2-15 所示。

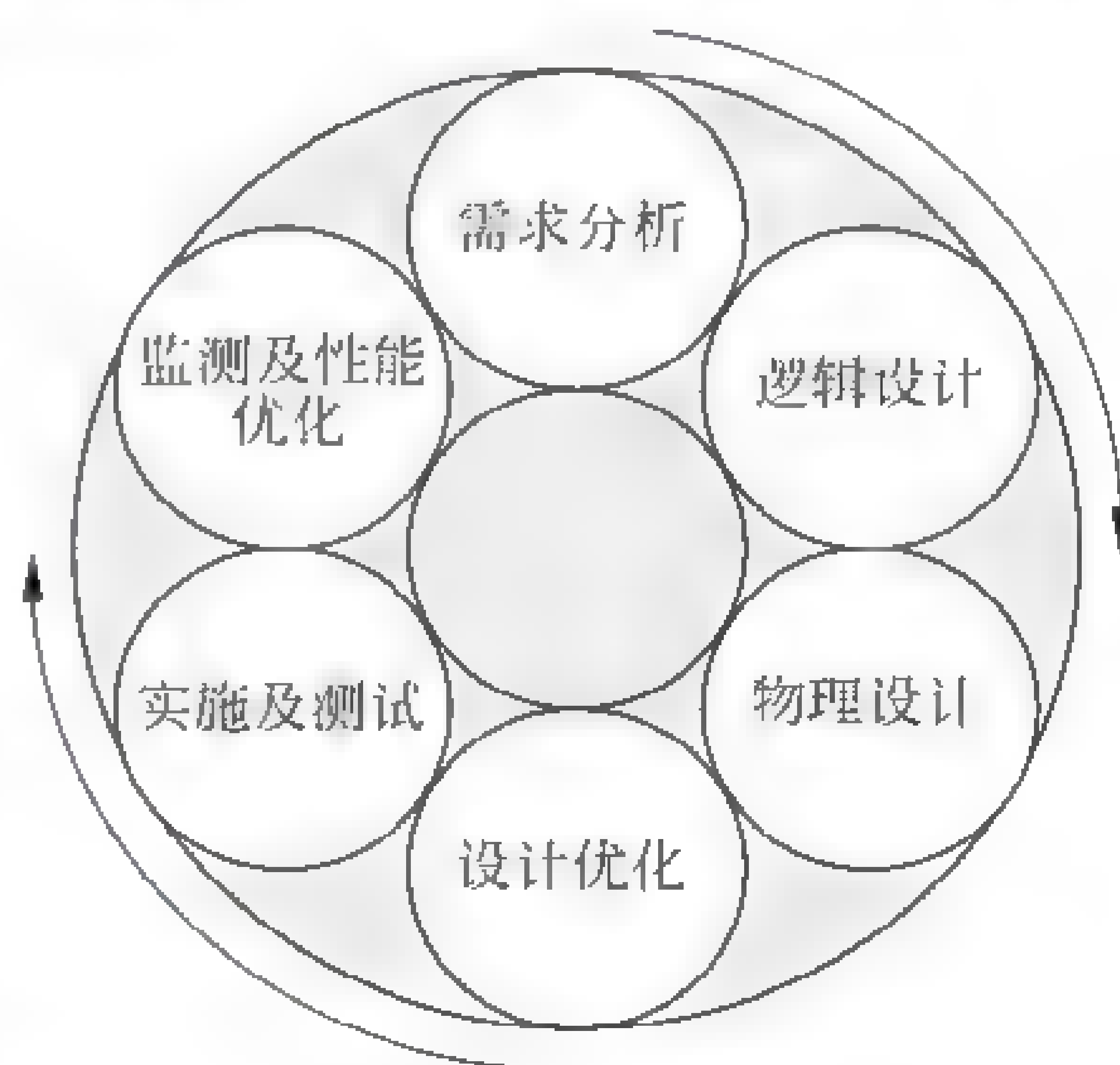


图 2-15　六阶段周期

需求分析阶段，网络分析人员通过与用户和技术人员进行交流来获取用户对新的或升级系统的商业和技术目标，然后归纳出当前网络的特征，分析出当前和将来的网络通信量、网络性能，包括流量、负载、协议行为和服务质量要求。

逻辑设计阶段，主要完成网络的逻辑拓扑结构、网络编址、设备命名、交换及路由协议选择、安全规划、网络管理等设计工作，并且根据这些设计产生对设备厂商、服务提供商的选择策略。

物理设计阶段，根据逻辑设计的成果，选择具体的技术和产品，使得逻辑设计成果符合工程设计规范。

设计优化阶段，该阶段完成在实施阶段前的方案优化，通过召开专家研讨会、搭建试验平台、网络仿真等多种形式，找出设计方案中的缺陷，并进行方案优化。

实施及测试阶段，该阶段根据优化后的方案进行设备的购置、安装、调试与测试，通过测试和试用，发现网络环境与设计方案的偏离，纠正实施过程中的错误，甚至可能导致修改网络设计方案。

监测及性能优化阶段，该阶段是网络的运营和维护阶段，通过网络管理、安全管理等技术手段，对网络是否正常运行进行实时监控，一旦发现问题，通过优化网络设备配置参数，达到优化网络性能的目的；一旦发现网络性能已经无法满足用户需求，则进入下一次迭代周期。

六阶段周期偏重于网络的测试和优化，侧重于网络需求的不断变更，由于其严格的逻辑设计和物理设计规范，使得该种模式适合于大型网络的建设工作。

2.2.3 网络开发过程

网络开发过程描述的是在开发一个网络时必须完成的基本任务，而网络生命周期的迭代模型为描绘网络项目的开发提供了特定的理论模型，因此网络开发过程主要是指一次迭代过程。

由于一个网络项目从构思到最终退出应用，一般会遵循迭代模型，经历多个迭代周期，而每个周期的各种工作可根据新网络的规模采用不同的迭代周期。例如在网络建设初期建设的是试点网络，由于网络规模比较小，因此第一次迭代周期的开发工作采用四阶段方式；而随着应用的发展，需要基于试点网络的建设，进行全面网络建设和互联，则扩展后的网络规模较大，则可以在第二次迭代周期中采用五阶段或六阶段方式。

由于网络工程中，中等规模的网络较多，并且应用范围较广，因此在后续的章节中，主要介绍的是五阶段迭代周期方式，该方式也适用于部分应用要求、覆盖要求比较单纯的大型网络。在较为复杂的大型、超大型网络中，采用六阶段周期时，也必须完成五阶段周期中要求的各项工作，只是增强了灵活性和必需的验证机制。

将大型问题分解为多个小型可解的简单问题，这是解决复杂问题的常用方法，根据五阶段迭代周期的模型，网络开发过程可以被划分为5个阶段，这5个阶段是：

- 需求分析。
- 现有的网络体系分析，即通信规范分析。
- 确定网络逻辑结构，即逻辑网络设计。
- 确定网络物理结构，即物理网络设计。
- 安装和维护。

因此网络工被分解成为多个容易理解、容易处理的部分，每个部分的工作都是一个阶段，各阶段的工作成果都将直接影响到下一阶段工作的开展，这就是五阶段周期被称为流水线的真正含义。

在这 5 个阶段中，每个阶段都必须依据上一阶段的成果，完成本阶段的工作，并形成本阶段的工作成果，作为下一阶段的工作依据；这些阶段成果分别为“需求规范”、“通信规范”、“逻辑网络设计”、“物理网络设计”。例如，在需求分析阶段，需要一份关于软件、硬件、连接和服务的详细说明书，以确保满足每个项目各自的独特需求；只有在网络计划者已经分析和确定了现有网络体系结构、新的需求、设计目标和约束，并形成了需求规范后才能开始后续设计工作。这样，在大多数大中型网络开发过程中，网络开发过程就可以用图 2-16 描述。

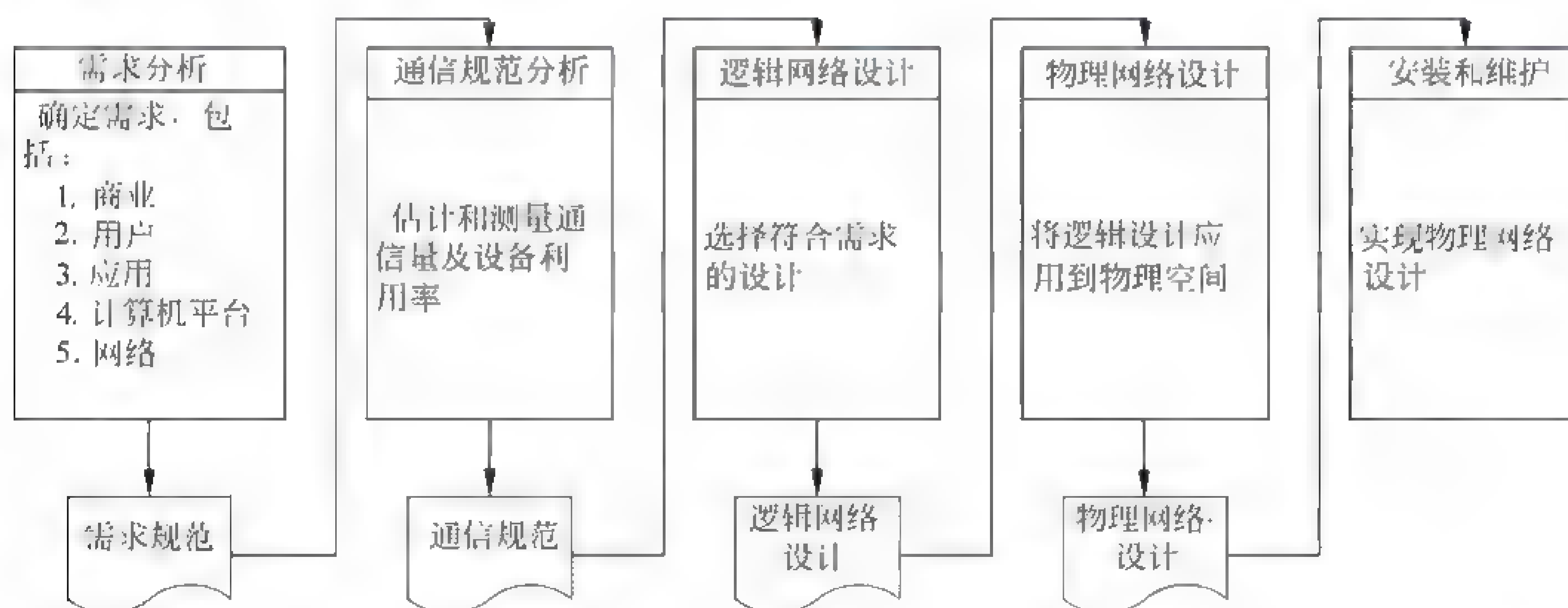


图 2-16　五阶段网络开发过程

各阶段的输出成果将直接关系到下一阶段的工作，因此作为工作成果的产物，包括所有记录设计规划、技术选择、用户信息以及上级审批的文件都应该保存好，以便以后查询和参考；另外，在极端情况下，如果某一阶段的工作出现重大失误，可以根据上一阶段成果，重新执行本阶段的工作。

下面介绍网络开发过程的各个阶段，只有理解了开发网络项目的各个阶段，才可以在实际开发过程中灵活运用。

1．需求分析

需求分析是开发过程中最关键的阶段，所有的工程设计人员都清楚，如果在需求分析阶段没有明确需求，则会导致以后各阶段的工作严重偏移。需求阶段需要直接面对的就是需求收集的困难，很多时候甚至用户自己也不清楚具体需求是什么，或者需求渐渐增加而且经常发生变化，需求调研人员必须采用多种方式与用户交流，才能挖掘出网络工程的全面需求。

收集需求信息不仅要和不同的用户、经理和其他网络管理员交流，而且需要把交流所得信息归纳解释。在这个过程中，很容易出现不同用户群体之间的需求矛盾，尤其是网络用户和网络管理员之间的分歧，网络用户总是希望能够更多、更方便地享用网络资源，而网络管理员则更希望网络稳定、用户管理方便， 需求出现矛盾其实是正常的，这也说明需求调查是全面的。设计人员只需要在设计工作中根据工程经验，均衡考虑各方利益，不激化用户矛盾，就能保证最终的网络是可用的。

收集需求信息是一项费时的工作，也不可能很快产生非常明确的需求，但是可以明确需求变化的范围，通过网络设计的伸缩性保证网络工程满足用户的需求变化；所以，需求分析有助于设计者更好地理解网络应该具有什么功能和性能，最终设计出符合用户需求的网络，它为网络设计提供了下述的依据：

- 能够更好地评价现有的网络体系。
- 能够更客观地做出决策。
- 提供完美的交互功能。
- 提供网络的移植功能。
- 合理使用用户资源。

不同的用户有不同的网络需求，收集需求时考虑如下：

- 业务需求。
- 用户需求。
- 应用需求。
- 计算机平台需求。
- 网络需求。

在需求分析阶段应该尽量明确定义用户的需求。在需求分析阶段，如果网络工程较大，则可以将调查人员划分成若干个小组，每个小组的分工不同，但是定期讨论需求，找出调查需求的不一致处，通过对不一致处进行更细致调查，形成全面需求。另外，在需求调查的手段上，可以采用多种方式，例如对于大范围的调查，可以采用书面的调查问卷，收集调查问卷并统计；对于相似的用户群，可以采用抽样访谈的方式，通过直接的交流，获取用户的特定需求。

详细的需求描述使得最终的网络更有可能满足用户的要求。同时，需求收集过程必须同时考虑现在和将来的需要，如不适当考虑将来的发展，以后将会很难实现对网络的

扩展。

最后，需要注意的是需求分析的输出是产生一份需求说明书，也就是需求规范。网络设计者必须规范地把需求记录在一份需求说明书中，清楚而细致地总结单位和个人的需要和愿望。在写完需求说明书后，管理者与网络设计者应该正式达成共识，并在文件上签字，这是规避网络建设风险的关键。这时需求说明书才成为开发小组和管理者之间的协议，也就是说，管理者认可文件中对他们所要系统的描述，网络开发者同意提供这个系统。

在形成需求说明书之前，网络工程设计人员还必须与网络管理部门就需求的变化建立起需求变更机制，明确允许的变更范围。这些内容正式通过后，开发过程就可以进入下一个阶段了。

2．现有的网络体系分析

如果说当前网络开发过程不是第一次迭代周期，也就是说已经存在一个网络，当前周期是对现有网络的升级和改造时，就必须添加现有网络体系分析工作。现有网络体系分析工作的目的是描述资源分布，以便于在升级时尽量保护已有投资，通过该工作，可以使网络设计者掌握网络现在所处的状态和情况。

升级后的网络效率和当前网络中的各类设备资源是否满足新需求是相关的，如果现有的网络设备不能满足新的需求，就必须淘汰并购置新的设备。因此，在写完需求说明书后，在设计过程开始之前，必须彻底分析现有网络和新网络相关的各类资源。

在这一阶段，应给出一份正式的通信规范说明文档，作为下一个阶段（逻辑网络设计）的输入使用。网络分析阶段应该提供的通信规范说明文档内容如下：

- 现有网络的逻辑拓扑图。
- 反映网络容量、网段及网络所需的通信容量和模式。
- 详细的统计数据、基本的测量值和所有其他直接反映现有网络性能的测量值。
- Internet 接口和广域网提供的服务质量（QoS）报告。
- 限制因素列表清单，例如，使用线缆和设备等。

3．确定网络逻辑结构

网络逻辑结构设计是体现网络设计核心思想的关键阶段，在这一阶段根据需求规范和通信规范，选择一种比较适宜的网络逻辑结构，并基于该逻辑结构，实施后续的资源分配规划、安全规划等内容。

网络的逻辑结构设计，来自于用户需求中描述的网络行为、性能等要求，逻辑设计要根据网络用户的分类、分布，形成特定的网络结构，该网络结构大致描述了设备的互联及分布，但是不对具体的物理位置和运行环境进行确定。

由于网络划分为多个层次，因此相同的一个网络设备连接图，在不同的网络协议层次上，其连接图是不同的，尤其是在网络层和传输链路控制层；而逻辑网络设计阶段，设计人员一般更关注于网络层的连接图，因为这涉及网络互联、地址分配、网络层流量

的关键因素。

网络设计者利用需求分析和现有网络体系分析的结果来设计逻辑网络结构。如果现有的软、硬件不能满足新网络的需求，现有系统就必须升级。如果现有系统能够继续运行使用，可以将它们集成到新设计中来。如果不集成旧系统，网络设计小组可以找一个新系统，对它进行测试，确定是否符合用户的需求。

此阶段最后应该得到一份逻辑网络设计文档，输出的内容包括以下几点。

- 逻辑网络设计图。
- IP 地址方案。
- 安全方案。
- 具体的软硬件、广域网连接设备和基本的服务。
- 招聘和培训网络员工的具体说明。
- 对软硬件、服务、员工和培训的费用的初步估计。

4．确定网络物理结构

物理网络设计是对逻辑网络设计的物理实现，通过对设备的具体物理分布、运行环境等的确定，确保网络的物理连接符合逻辑连接的要求。在这一阶段，网络设计者需要确定具体的软硬件、连接设备、布线和服务。

如何选择和安装设备，由网络物理结构这一阶段的输出作依据，所以网络物理结构设计文档必须尽可能详细、清晰，输出的内容如下：

- 网络物理结构图和布线方案。
- 设备和部件的详细列表清单。
- 软硬件和安装费用的估算。
- 安装日程表，详细说明服务的时间以及期限。
- 安装后的测试计划。
- 用户的培训计划。

5．安装和维护

第 5 个阶段可以分为两个小阶段，分别是安装和维护。

1）安装

安装阶段是根据前面各个阶段的工程成果，实施环境准备、设备安装调试的过程。

安装阶段的主要输出是网络本身。好的安装阶段应该产生的输出如下：

- 逻辑网络图和物理网络图，以便于管理人员快速掌握网络。
- 满足规范的设备连接图、布线图等细节图，同时包括线缆、连接器和设备的规范标识，这些标识应与各细节图保持一致。
- 运营维护记录和文档，包括测试结果和新的数据流量记录。

在安装开始之前，所有的软硬件资源必须准备完毕，并通过测试。在网络投入运营之前，人员、培训、服务、协议等都是必须准备好的资源。

2）维护

网络安装完成后，接受用户的反馈意见和监控是网络管理员的任务。网络投入运行后，需要做大量的故障监测和故障恢复以及网络升级和性能优化等维护工作。网络维护又称为网络产品的售后服务。

2.2.4　网络设计的约束因素

网络设计的约束因素不同于网络设计目标，是网络设计工作必须遵循的一些附加条件，一个网络设计，即使可以达到设计的目标，但是由于不满足约束条件，将导致该网络设计无法实施。所以，在需求分析阶段，在确定用户需求的同时，也应对这些附加条件进行明确。

在一个网络工程中，满足用户需求的网络设计是一个集合，设计因素就是过滤条件，而过滤后的设计集合，就是可以实施的设计集合。

一般来说，网络设计的约束因素主要来自于政策、预算、时间和应用目标检查方面。

1．政策约束

了解政策约束的目标是发现隐藏在项目背后的可能导致项目失败的事务安排、持续的争论、偏见、利益关系或历史等因素。政策约束的来源包括法律、法规、行业规定、业务规范、技术规范等，政策约束的直接体现是法律法规条文、发表的暂行规定、国际国家行业标准、行政通知与发文等。

在网络开发中，设计人员需要与客户就协议、标准、供应商等方面的政策进行讨论，弄清楚客户在传输、路由选择、桌面或其他协议方面是否已经制定了标准，是否有关于开发和专有解决方案的规定，是否有认可供应商或平台方面的相关规定，是否允许不同厂商之间的竞争。在明确了这些政策约束后，才能开展后期的设计工作，以免出现设计失败或重复设计的现象。

需要特别注意的是，对于一个已经进行过但没有成功的类似项目，应当判断类似的情况是否有可能再次发生，采取什么方案才能避免。

2．预算约束

预算是决定网络设计的关键因素，很多满足用户需求的优良设计，就是因为突破了用户的基本预算而不能实施。

如果用户的预算是弹性的，那就意味着赋予了设计人员更多的空间，设计人员可以从用户满意度、可扩展性、易维护性等多个角度对设计进行优化；但是大多数情况下，设计人员面对的是刚性的预算，预算可调整的幅度非常小，在刚性预算下实现满意度、可扩展性、易维护性是需要大量工程设计经验的。

需要注意的是，对于预算不能满足用户网络需求的情况，放弃网络设计工作并不是一种积极的态度，正确的做法，是在统筹规划的基础上，将网络建设工作划分为多个迭代周期，同时将网络建设目标分解为多个阶段性目标，通过阶段性目标的实现，到达最

终满足用户全部需求的目的，而当前预算仅用于完成当前迭代周期的建设目标。

预算的正确分解也是需要面对的工作，网络预算一般分为一次性投资预算和周期性投资预算，一般来说年度发生的周期性投资预算和一次性投资预算之间的比例为10%～15%是比较合理的。一次性投资预算主要用于网络的初始建设，包括设备采购、购买软件、维护和测试系统，培训工作人员以及设计和安装系统的费用等；应根据一次性投资预算，对设备、软件进行选型，对培训工作量进行限定，确保网络初始建设的可行性。周期性投资预算主要用于后期的运营维护，包括人员消耗、设备维护消耗、软件系统升级消耗、材料消耗、信息费用、线路租用费用等多个方面；同时，对客户单位的网络工作人员的能力进行分析，考察他们的工作能力和专业知识是否能够胜任以后的工作，并提出相应的建议，是评判周期性投资预算是否能够满足运营需要的关键之一。

最后，评判多个相同或近似预算网络工程的优劣，还要对网络的投资回报进行分析，从降低运行费用、提高劳动效率、扩大市场等多个角度来选择最适合的网络建设方案。

3．时间约束

网络设计的进度安排是需要考虑的另一个问题。项目进度表限定了项目最后的期限和重要的阶段。通常，项目进度是由客户负责管理，但网络设计者必须就该日程表是否可行提出自己的意见。

有许多种开发进度表的工具，在全面了解了项目之后，要对网络设计者自行安排的计划与进度表的时间进行对照分析，对于存在疑问的地方，要及时与客户进行沟通。

4．应用目标检查

在进行下一阶段的任务之前，需要确定是否了解了客户的应用目标和所关心的事项。通过应用目标检查，可以避免用户需求的缺失，检查形式包括设计小组内部的自我检查和用户信息主管部门的确认检查两种。常用的应用检查项目包括：

- 对客户所处的产业和竞争情况做的调查。
- 对客户公司结构的了解情况。
- 编制了客户商业目标清单，明确了网络设计的最主要目的。
- 客户对所有关键任务操作的明确程度。
- 客户对成功和失败的衡量标准。
- 网络设计项目的范围。
- 客户的网络应用。
- 客户已就认可的供应商、协议、平台等政策进行的解释。
- 客户已就网络设计和实现的分布授权的相关政策进行的解释。
- 对项目预算的了解。
- 对项目进度的安排，包括最后期限和重要阶段以及进度安排符合实际。
- 对客户和相关的内部、外部工作人员的技术知识的了解。
- 就员工培训计划进行的探讨。

- 注意到了可以影响网络设计的办公策略。

在明确了设计人员对以上内容都已经清楚，并且与用户不存在分歧之后，才可以进行下一阶段的设计工作。

需要注意的是，在网络设计工作中，由于用户的不同群体存在着不同的需求和约定，经常会出现约束条件冲突的情况，这些约束条件的冲突问题可以依据两种思路来解决，一是由用户的信息主管部门协调解决，一是针对冲突的约束条件排定优先级，优先满足最高级别的约束条件。

2.3 网络需求分析

网络需求分析是网络开发过程的起始部分，在该阶段，应明确客户所需的网络服务和性能。本小节介绍了需求收集分析的过程，并描述了如何编制需求说明书。

2.3.1 需求分析的必要性

需求分析是用来获取网络系统需求和业务需求的方法，该过程是网络开发的基础，也是开发过程中的关键阶段。

虽然网络需求分析不同于软件应用系统的需求分析工作，但是网络设计人员也需要与用户进行大量的交流和沟通，也需要通过对用户业务流程的了解来细化网络需求。一般来说，如果网络工程是和应用软件同时进行的，则可以将网络需求调查和应用软件的需求调查结合在一起进行。通过多种沟通手段，使得设计人员不仅了解了用户的业务知识，同时了解用户对网络的基本需求，为后续步骤建立一个稳固的工作基础。

需求分析工作为设计者提供了以下的设计依据：

- 能够更好地评价现有的网络体系。
- 能够更客观地做出决策。
- 提供完美的交互功能。
- 提供网络的移植功能。
- 合理使用用户资源。

在需求分析阶段对用户需求的定义越明确和详细，则实施期间需求变动的可能性就越小，同时建设后网络的用户满意度就越高。

2.3.2 收集需求分析的过程

在需求分析过程中，需要考虑以下几个方面的需求：

- 业务需求。
- 用户需求。
- 应用需求。

- 计算机平台需求。
- 网络需求。

2.3.2.1 业务需求

1. 建立业务需求

在整个网络开发过程中，业务需求调查是理解业务本质的关键，应尽量保证设计的网络能够满足业务的需求。

网络工程是为一个集体提供网络服务的，在这个集体中，存在着职能的分工，也存在着不同的业务需求，一般来说用户只对自己分管的业务需求非常清晰，对于其他用户的需求会产生侧面的了解，因此对于集体内的不同用户，都需要收集特定的业务信息，这些信息包括以下内容。

1）确定主要相关人员

业务需求收集的第一步是获取组织机构图，通过组织机构图了解集体中的岗位设置以及岗位职责，典型的组织机构图如图 2-17 所示。

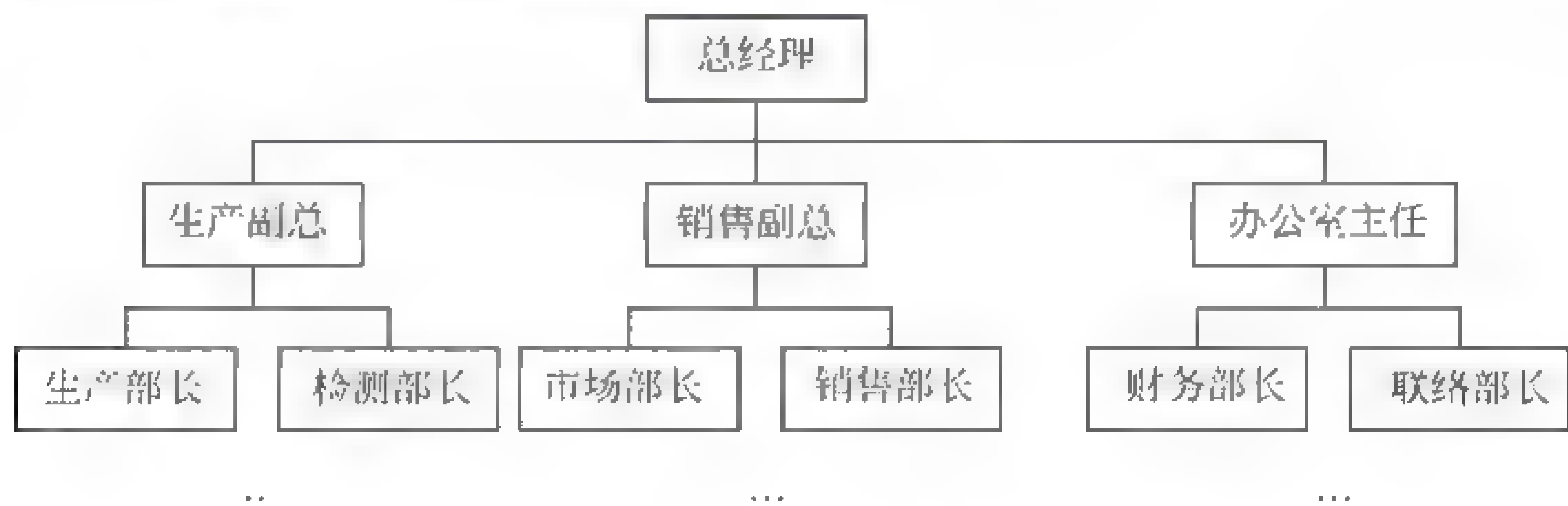


图 2-17 组织机构图

在调查组织机构的过程中，主要与以下两类人员重点沟通。

- 决策者：负责审批网络设计方案或决定投资规模的管理层。
- 信息提供者：负责解释业务战略、长期计划和其他常见的业务需求。

2）确定关键时间点

项目的时间限制是完工的最后期限，对于大型项目，必须制定严格的项目实施计划，确定各阶段及关键的时间点，同时这些时间点的产物也是重要的里程碑。在计划设定后，即形成项目阶段建设日程表，这个日程表在得到项目的更多信息后还可以更进一步细化。

3）确定网络的投资规模

对于整个网络的设计和实施，费用是一个主要考虑的因素，投资规模将直接影响到网络工程的设计思路、技术路线、设备购置、服务水平。

面对确定的网络规模，投资的规模也必须合理并符合工程要求，存在一个投资最低限额；如低于该限额，则会出现资金缺乏等问题，导致网络建设失败。

在进行投资预算或者预算确认时，应根据工程建设内容进行核算，将一次性投资和周期性投资都纳入考虑范围，并据实向管理层汇报费用问题。

计算系统成本时，有关网络设计、实施、维护和支持的每一类成本都应该纳入考虑中。表 2-3 所示的是需要考虑的投资项目清单，可根据项目实际情况进行调整。

表 2-3　投资项目清单

投 资 项 目	投 资 子 项	投 资 性 质
核心网络	核心网络设备	一次性投资
	核心主机设备	一次性投资
	核心存储设备	一次性投资
会聚网络	会聚网络设备	一次性投资
接入网络	接入网络设备	一次性投资
综合布线	综合布线	一次性投资
机房建设	机房装修	一次性投资
	UPS	一次性投资
	防雷	一次性投资
	消防	一次性投资
	监控	一次性投资
平台软件	数据库管理软件	一次性投资
	应用服务器软件	一次性投资
	各类中间件软件	一次性投资
	工作流软件	一次性投资
	门户软件	一次性投资
软件开发	应用软件产品购置	一次性投资
	应用软件开发	一次性投资
	门户开发	一次性投资
安全设备	核心安全设备	一次性投资
	边界安全设备	一次性投资
	桌面安全设备	一次性投资
系统管理	网络管理软件	一次性投资
	安全管理软件	一次性投资
	桌面管理软件	一次性投资
	应用管理软件	一次性投资
实施管理	集成	一次性投资
	测试	一次性投资
	评测	一次性投资
	培训	一次性投资
	监理	一次性投资

续表

投 资 项 目	投 资 子 项	投 资 性 质
运营维护费用	通信线路费	周期性投资
	设备维护费	周期性投资
	材料消耗费	周期性投资
	人员消耗费	周期性投资
不可预见费用		一次性投资

4）确定业务活动

在设计一个网络项目之前，应通过对业务活动的了解，来明确网络的需求。一般情况下，网络工程对业务活动的了解并不需要非常细致，主要是通过对业务类型的分析，形成各类业务对网络的需求，主要包括最大用户数、并发用户数、峰值带宽、正常带宽等。

5）预测增长率

预测增长率是另一类常规需求，通过对网络发展趋势的分析，明确网络的伸缩性需求。

预测增长率主要考虑以下方面的网络发展趋势：

- 分支机构增长率。
- 网络覆盖区域增长率。
- 用户增长率。
- 应用增长率。
- 通信带宽增长率。
- 存储信息量增长率。

预测增长情况主要采用两种方法，一是统计分析法，一种是模型匹配法。统计分析法是基于该网络前若干年的统计数据，形成不同方面的发展趋势，最终预测未来几年的增长率。模型匹配法是指根据不同的行业、领域建立各种增长率的模型，而网络设计者根据当前网络的情况，依据经验选择模型，对未来几年的增长率进行预测。需要注意的是，只有对于网络比较复杂、发展变化较大的网络工程，才需要进行预测增长率。

6）确定网络的可靠性和可用性

网络的可用性和可靠性需求是非常重要的，甚至这些指标的参数可能会影响到网络的设计思路和技术路线。

一般来说，不同的行业拥有自己的可用性、可靠性要求，网络设计人员在进行需求分析过程中，应首先获取行业的网络可靠性和可用性指标标准，并基于该标准与用户进行交流，明确特殊要求。这些特殊的要求甚至可能是可用性达到 7×24 小时、线路故障后立即完成备用线路切换，并不对应用产生影响等非常苛刻的需求。

7）确定 Web 站点和 Internet 的连接性

Web 站点可以自己构建，也可以由网络服务提供商提供，无论采用哪种方式，一个集体的 Web 站点或内部网络在设计时总是反映了其自身的业务需求。只有完全理解了一个组织的 Internet 业务策略，才可能设计出具有可靠性、可用性和安全性的网络。

8）确定网络的安全性

确定网络的安全性需求，构建合适的安全体系是网络设计工作的保证。在网络设计方面，存在着很多误区，无论是过分强调网络的安全性，还是对网络安全不屑一顾，都是不合适的设计思路。正确的设计思路是调查出用户的信息分布，对信息进行分类，根据分类信息的涉密性质、敏感程度、传输与存储、访问控制等安全要求，确保网络性能和安全保密的平衡。

对大多数网络来说，由于用户的信息多是非涉密的信息，因此提供普通的安全保障技术措施就可以了；但对于有特殊业务，网络中存在涉密、敏感信息的网络，例如级别较高的政府部门或进行有关国家安全的高度机密开发工作的公司，其网络所承载的业务就需要对职员进行严格的安全限制，使用严格的手续来保证信息的安全访问和输出。

网络安全需求调查中最关键的一点是，不能出现网络安全需求的扩大化，提倡适度安全。

9）确定远程访问

远程访问是指从互联网或者外部网络访问内部网络、企业网络，当网络用户不在企业或组织网络内部时，可以借助于加密技术、VPN 等技术，从远程网络来访问内部网络。通过远程访问，可以实现在任意时间、地点都可工作的需求，这也需要配置相应的远程访问安全技术要求。

根据需求分析，网络设计者要确定网络是否具有远程访问的功能，或是根据网络的升级需要，考虑网络的远程访问。

2．输出——业务需求清单

设计人员与各类人员通过多种形式的交流，获取了组织内部的业务需求，这些业务需求主要通过文档的形式体现，绝大多数业务需求文档都应包含如下的内容：

（1）确定主要相关人员。

- 信息来源。
- 信息管理人员名单。
- 相关人员的联系方式。

（2）确定关键时间点。

- 项目起始时间点。
- 项目的各阶段时间安排计划。

（3）确定工程投资规模。

- 投资规模估算。
- 预算费用估算。

（4）业务活动。
- 业务分类。
- 各类业务的网络需求。

（5）预测增长率。
- 分支机构增长率。
- 网络覆盖范围增长率。
- 用户增长率。
- 应用增长率。
- 通信带宽增长率。
- 存储信息增长率。

（6）网络的可靠性和可用性。
- 业务活动的可靠性要求。
- 业务活动的可用性要求。

（7）确定 Web 站点和 Internet 的连接性。
- Web 站点栏目设置。
- Web 站点的建设方式。
- 网络的 Internet 出口要求。

（8）确定网络的安全性。
- 信息保密等级。
- 信息敏感程度。
- 信息的存储与传输要求。
- 信息的访问控制要求。

（9）确定远程访问。
- 远程访问要求。
- 需要远程访问的人员类型。
- 远程访问的技术要求。

在输出清单中，还应该特别记录管理层人员对新网络设计的基本需求，以及管理层列出的该系统所需的特殊功能。预先详细考虑新系统的特殊性能将会使以后的工作效率得到大大的提高，除此之外还能增强竞争力，减少费用开支。

2.3.2.2 用户需求

1．收集用户需求

收集用户需求应从当前的网络用户开始，找出用户需要的重要服务或功能；对用户需要的功能进行分析，区分出单机服务、网络服务；对于网络服务，还要根据服务的性质和用户的设想，区分交互式服务、C/S 服务、BPS 服务等。

为了设计出符合用户需求的网络，收集用户需求过程应从当前的网络用户开始，必

须找出用户需要的重要服务或功能。这些服务可能需要网络完成，也可能只需要本地计算机完成。例如有些用户服务属于局部应用，由本机的应用程序提供，只须使用用户计算机和外围设备，而其他服务则需要通过网络连接，由工作组服务器、大型机或 Web 服务器提供。在很多情况下，可通过其他备选方案来满足用户需要的服务。

收集用户需求的过程中，需要注意与用户的交流，网络设计者应将技术性语言转化为普通的交流性语言，并且将用户描述的非技术性需求转换为特定的网络属性要求，例如网络带宽、并发连接数、每秒新增连接数等。

2．收集需求的机制

用户需求收集的机制，主要包括与用户群的交流、用户服务、需求归档三个方面。

1）与用户群交流

与用户交流指与特定的个人和群体进行交流。在交流之前，需要先要确定这个组织的关键人员和关键群体，再实施交流。在整个设计和实施阶段，应始终保持与关键人员之间的交流，以确保网络工程建设不偏离用户需求。

在网络开发过程中，都要注意与用户群交流的方法和技巧，应该避免交流不充分和交流过于频繁。避免交流不充分，关键是主要交流的方式和人员，找到正确、对业务非常清晰的人既可以减少交流的工作量，也可以避免由于过量而无用的信息导致设计出现的偏差；通常这些熟悉业务，并有一定归纳能力的人，都被称为行业专家，他们对网络设计的影响和组织的领导人员是等同的；另外，交流的方式也非常重要，应针对不同的人员采用不同的交流方式，例如对于一线工作人员，你可以采用先下发调查问卷，再依据调查问卷进行访谈的方式。避免交流过于频繁的关键在于每次交流前都要有明确的交流目标，同时交流后的归纳和总结同样可以提高交流的效率，否则就会使管理层和用户群体在项目结束前就厌烦听到有关网络开发的细节，从而产生抵触情绪，给工作带来麻烦。

收集用户需求的三种最常用的方式如下。

（1）观察和问卷调查。

对于一个工作性质相同的用户群体，观察和问卷调查是成本较低、成效快捷的收集用户需求方式。问卷的制作应简单、可操作性强，尽量使用选择方式，而不是让用户填写大段的文字；而观察工作，重点是注意用户对各类信息、报表、文件的处理。

另外，问卷调查的方式还可以根据用户的情况进行调整：对于计算机操作能力不强的用户群，只能采用下发调查问卷，并录入调查结构的方式；对于计算机操作能力很强的用户群，可以采用下发电子文档或者开发调查网页的方式，简化调查结果录入工作。

（2）集中访谈。

不管是否进行大规模的问卷调查，集中访谈方式都是不能忽略的；对于不需要进行问卷调查的小规模网络工程，则可以直接将用户代表集中起来进行讨论，明确需求；对于进行了问卷调查的大规模网络工程，则需要对问卷调查结果进行分析，抽取部分用户

代表，就问卷形式无法解决的问题进行讨论，从而发现深层次的问题。

（3）采访关键人物。

采访关键人物虽然涉及的人员较少，整体工作量较小，但是由于这些关键人物对网络工程的影响力，其访谈的准备工作和总结工作是非常重要的。一般来说这些关键人物主要是各级领导和行业专家，各级领导主要从管理角度明确需求，而行业专家则明确的是业务需求。

采访关键人物之前，一定要有针对地制定问题提纲，并最好先将提纲发给被采访人员；在采访过程开始前，应首先获取联系方式，最好和访谈者约定邮件、电话、即时通信机制；对关键人物不可能一次访谈就明确了所有需求，但是第一次访谈一定要形成需求的大致框架，以便于后期访谈工作的开展。

2）用户服务

除了信息化程度很高的用户群体，大多数用户都不可能用计算机的行业术语来配合设计人员的用户需求收集。设计人员不仅要将问题转化成为普通业务语言，也应从用户反馈的业务语言中提炼出技术内容，这需要设计人员有大量的工程经验和需求调查经验。

一般来说，用户描述的需求总是主观且可变的，与用户的信息化程度、经验和环境有很大的关系。需求收集人员需要注意以下方面内容的表述，否则很容易形成需求的偏离。

（1）信息的及时传输。

及时传输能使用户快速访问、传输或修改信息，它主要取决于用户对系统时间的需求。但是用户在描述及时传输性时，是很难用量化的时间来描述的，通常听到的话是“传输得够快”、“不要太慢”等，这需要调查人员引入参照物，例如“像访问××网站那样快”，从而对及时传输要求进行量化。

（2）响应时间的可预测。

用户对响应时间的预测，是基于响应时间不能影响其业务工作，需求收集人员对每个业务的响应时间需求的明确，可以通过对现有业务时间的调查来形成参照。例如，在门诊挂号系统中，每次挂号的响应不能长于现有人工挂号的平均时间。

（3）可靠性和可用性。

可靠性和可用性也是紧密相关的，用户很难区分可靠性、可用性、可恢复性等概念，他们只会通过一些用户体验性语言来进行描述，例如“这个系统是不能停机的”、“系统在出故障后，应该在一个小时内就能恢复”，需求收集人员应提炼出对可靠性、可用性等特定的参数指标。

（4）适应性。

适应性是系统适应用户改变需求的能力，用户只会提出特定的服务要求，而不会去关心服务是如何在网络中实现的，例如网络用户希望网络中有一台 FTP 服务器，以便于进行文件的上下载，但是大多数人是不会关心这台服务器存放的位置、采用的操作系统、

FTP 服务器软件的版本等信息。需求收集人员主要是收集用户的服务要求，而暂时不用考虑如何实现，这是设计阶段的任务。

（5）可伸缩性。

从用户的角度来看，可伸缩性通常不是在面谈和调查用户时获得的信息，而是通过估计公司预期的增长率而得到的。

（6）安全性。

安全性保证用户所需的信息和物理资源的完整性，但大多数用户很难正确描述安全的需求，所以需求调查人员的引导非常重要，要针对应用和信息的需要来正确建议安全技术。

（7）低成本。

低成本意味着实现相同的功能而花的费用相对少，这是用户所期待的，也是网络设计者在开发网络项目时应该追求的目标之一。

3）需求归档机制

与其他所有技术性工作一样，必须将网络分析和设计的过程记录下来。文档有助于将需求用书面形式记录下来便于保存和交流，也有利于今后说明需求和网络性能的对应关系。所有的访谈、调查问卷等最好能由用户代表进行签字确认，同时应根据这些原始资料整理出规范的需求文档。

3．输出用户服务表

用户服务表可用于收集和归档需求类型信息，也可用来指导管理人员和网络用户的讨论。用户服务表主要是需求服务人员自行使用的表格，不面向用户，类似于备忘录，在收集用户需求时，应利用用户服务表随时纠正收集工作的失误和偏差。

用户服务表没有固定的格式，各设计团队可以根据自己的经验自行设计用户服务表，表 2-4 是一个简单的示例。

表 2-4　用户服务列表

用户服务需求	服务或需求描述
地点	
用户数量	
今后 3 年的期望增长速度	
信息的及时发布	
可靠性/可用性	
安全性	
可伸缩性	
成本	
响应时间	
其他	

2.3.2.3 应用需求

1. 收集应用需求

应用需求收集工作应考虑如下因素：

- 应用的类型和地点。
- 使用方法。
- 需求增长。
- 可靠性和可用性需求。
- 网络响应。

这些需求因素的收集工作，通常可以从两个角度来完成，一是从应用类型自身的特性角度，另一个是从应用对资源的访问角度。

2. 应用类型

应用的种类较多，其中常见的分类方式主要有 4 种：

- 按功能分类。
- 按共享分类。
- 按响应分类。
- 按网络模型分类。

1）按功能分类

按功能对应用进行分类，则可以将应用划分为常见功能类型和特定功能类型。

常见功能类型的应用如图 2-18 所示，这些应用类型中的大多数都是日常工作中接触较为频繁，应用范围较广的。



图 2-18 常见功能类型应用

特定功能类型应用主要用于实现特定功能或面向特定工作。特定功能软件包括控制、维护网络和计算机系统的功能，例如防病毒软件和网络管理系统等；面向特定工作的工具软件主要是行业软件，包括金融计划系统、工程和设计应用、制造控制系统、排版工具等专业软件。

对应用需求按功能分类，依据不同类型的需求特性，可以很快归纳出网络工程中应用对网络的主体需求。

2）按共享分类

软件可根据其在网络中的用户数进行分类，分别为单用户软件、多用户软件和网络

软件。

单用户软件是运行于用户本地计算机的软件，在运行时只有一个用户可以访问，该软件进程只能访问本地资源，不能访问网络资源。虽然网络操作系统允许通过远程方式访问单机软件，但是该软件在运行时是不可能实现资源共享的。

多用户软件允许多个用户同时使用该软件，并且提供了用户间共享文件的机制。多用户软件通过分时机制、线程切换等多种机制实现多个用户并发，同时通过文件锁机制实现文件共享。多用户软件是借助于网络实现信息的存储和传递，因此需要更多的网络资源。

网络软件利用所有的网络资源，网络软件既可以集中安装在一台服务器上，也可以分布在不同的服务器上，是实现共享的最佳方式，借助于网络和应用协议来完成网络资源的共享。

网络内的应用软件总是沿着单用户软件→多用户软件→网络软件这条线索进行发展，随着共享程度的提高，会对网络提出更高的要求。

3）按响应分类

应用可以分为实时应用和非实时应用两种，不同响应方式具有不同的网络响应性能需求。

实时应用软件在收到信息后马上处理，一般不需要用户干涉，这对网络带宽、网络延迟等提出了明确的要求。在实时应用中，通常本地进程需要和远程进程保持同步，而且这些同步机制是固定周期发生的，因此实时应用要求信息传输的速率稳定，具有可预测性。

非实时应用更为广泛，非实时并不要求规定的同步机制，只是要求一旦发生请求，则需要在规定的时限内完成响应，因此对带宽、延迟的要求较低，但是对网络设备、计算机平台的缓冲区提出了较高的要求。

4）按网络模型分类

应用按网络处理模型，可以分为单机软件、对等网络软件、C/S 软件、BPS 软件、分布式软件。

- 单机软件指不访问网络资源的软件。
- 对等网络软件只运行于互联网内，不区分服务器和客户端的网络软件。
- C/S 软件指在网络中区分出服务器和客户端的网络软件系统。
- BPS 软件指划分了数据库服务器、应用服务器和客户端的网络软件系统，BPS 软件是三层模式、多层模式的典型代表。
- 分布式软件指调度网络中多个资源完成一个任务的网络软件系统。

应用采用不同的网络处理模型，会对网络产生不同的需求。

3．对资源的存取和访问

用户对应用系统的访问要求是网络设计的重要依据，网络工程必须保证用户可以非

常顺利地使用软件并获取需要的数据。用户对网络资源的存取和访问，是可以通过各种指标进行量化的，这些量化的指标通过统计产生，并直接反映了用户的需求。

需要考虑的指标包括以下一些：

- 每个应用的用户数量。
- 每个用户平均使用每个应用的频率。
- 使用高峰期。
- 平均访问时间长度。
- 每个事务的平均大小。
- 每次传输的平均通信量。
- 影响通信的定向特性。例如，在一个 C/S 软件系统中，客户端发送至服务器端的请求数据量非常小，但是服务器端返回的数据量较大。

4．其他需求

（1）增长率。

由于应用的发展，用户数量不断增长，因此对网络的需求也会随之变化。在获取应用需求时，需要询问用户对应用发展的要求或者规划。

（2）可靠性和可用性。

对网络的可靠性和可用性，除了从用户的角度获取需求之外，还要对网络中的应用进行分析，以便从技术角度对网络的可靠性和可用性需求进行补充；其需求收集的工作要点在于找出组织中重要应用系统的特殊可靠性和可用性需求，例如在公交公司的企业网络中，对公交车进行网络调度的软件，其可靠性和可用性需求就是重点。

（3）对数据更新的需求。

一个应用对信息更新的需求是由用户对最新信息的需求来决定的，但是用户对信息更新的要求，并不等同于应用对数据更新的需求。应用软件在面对相同的信息更新需求时，如果采用了不同的数据传输、存储技术，则会产生不同的数据更新需求，而网络设计直接面向数据更新需求。

5．输出——应用需求表

应用需求表概括和记录了应用需求的量化指标，这些量化指标会直接指导网络设计。表 2-5 为一个典型的应用需求表示例，可根据实际需要进行调整。

表 2-5 应用需求表

用户名	应用需求								
（应用程序名）	版本等级	描述	应用类型	位置	平均用户数	使用频率	平均事务大小	平均会话长度	是否实时

2.3.2.4　计算机平台需求

收集计算机平台需求是网络分析与设计过程中一个不可缺少的步骤，需要调查的计算机平台主要分为 5 类：

- 个人计算机。
- 工作站。
- 小型机。
- 中型机。
- 大型机。

1. 个人计算机

在计算机网络中，个人计算机（PC）已经不再简单地作为网络中的用户终端来使用了，由于 PC 服务器技术的不断发展，在很多应用中，PC 服务器逐步取代了专用服务器的作用和地位。

由于个人计算机是网络中分布最广、数量最多的节点，虽然技术含量较低，但是应该重点分析。在分析个人计算机需求时，应该考虑以下因素：

- 微处理器。
- 内存。
- 输入输出。
- 操作系统。
- 网络配置。

在设计网络时，用户会针对 PC 服务器提出最直接的需求，需求收集人员应根据需要进行各类因素的技术指标设计，在设计工作的后期形成设备的招投标技术参数。

1）微处理器

微处理器是反映个人计算机处理能力的关键部件，其性能主要体现在带宽和适中频率两个指标上。目前，个人计算机的微处理器主要是以 x86 系列为主，一般来说，应用于服务器上的微处理器和普通计算机的微处理器是存在差异的。

目前，微处理市场主要由几种产品构成，主流的是 x86 系列产品，同时也存在 Power PC 等产品。其中 x86 系列产品在指令位数进入 32 位后，主要的产品来自于 Intel、AMD 等公司。

2）内部存储器

内部存储器是衡量桌面系统性能的另一个重要指标。广义的内部存储器包括随机存储器（RAM）、高速缓存（cache）、磁盘缓存（HD cache）。

（1）随机存储器。

随机存储器是个人计算机的关键部件，所有软件都必须在装载至内存后，才能处于运行状态。RAM 的发展历经了 SIMM、SIMM FPM/EDO、DIMM　SDRAM、DIMM RAMBUS 等多个阶段。内存大小是选择个人计算机的指标。

（2）高速缓存。

高速缓存，有时也称为缓冲存储器或 RAM 缓存，指的是单独分出来存储常用指令的存储器的一部分。随着技术的发展，单纯的高速缓存已经不能满足用户的需求，产生了一级缓存、二级缓存、三级缓存的概念。一般来说，一级和二级缓存在 CPU 内部，三级缓存多存在于主板上。一级缓存的大小将直接决定程序的运行效率。

（3）磁盘缓存。

磁盘缓存的工作原理与高速缓存相同，它并不采用高速的 SRAM，而是传统的 RAM。磁盘缓存存在多种形式：一种是操作系统在内存中维持一个磁盘缓存区域，保证对磁盘的高速访问；另外是通过磁盘阵列卡上的 RAM 部件实现对磁盘数据缓存。

3）计算机总线

计算机总线技术的发展经历了 8 位 ISA 总线、16 位 ISA 总线、32 位 EISA 总线、64 位 PCI 总线，目前个人计算机或者服务器主要适用的 PCI 技术是 PCI-X 或者是 EPCI 技术。

4）操作系统

操作系统是影响个人计算机的主要因素之一，完成输入输出、用户交互、文件管理、进程管理等基本任务。目前个人技术上的操作系统以 Windows 和 UNIX 为主。

（1）Windows 操作系统。

微软（Microsoft）公司在 PC 操作系统市场占主导地位，曾依靠 DOS 操作系统打开市场，现在 Windows NT（Microsoft 公司的 32 位多任务操作系统）继续保持增长的趋势。微软的操作系统经历了 DOS、Windows 32、Windows 95/98、windows NT、Windows 2000、Windows XP、Windows 2003、Window Vista；目前普通计算机上的主流 Windows 操作系统为 Windows XP 和 Windows Vista，而服务器上主流 Windows 操作系统为 Windows 2003。

（2）UNIX 操作系统。

个人计算机上的 UNIX 操作系统较多，包括 Banyan VINES、SCO UNIX、Solaris、Linux，其中由芬兰赫尔辛基大学 Linus Torvalds 设计的 Linux 占据了主流地位，该操作系统基于自由源代码，符合标准操作系统界面（POSIX）的标准，是一种真正的多用户、多任务、可移植性好的操作系统。

目前应用较为广泛的中文版的 Linux 有以下几种：RedHat Linux、红旗 Linux、Turbo Linux、Xteam Linux、Tom Linux、COSIX Linux 等。

2．工作站

工作站是一种以个人计算机和分布式网络计算为基础，主要面向专业应用领域，具备强大的数据运算与图形、图像处理能力，为满足工程设计、动画制作、科学研究、软件开发、金融管理、信息服务、模拟仿真等专业领域而设计开发的高性能计算机。

工作站应用的领域主要包括以下一些方面：

- 计算机辅助设计及制造 CAD/CAM：这是工作站的传统领域，借助于运行图形工

作站上的 CAD/CAM 软件，可以直观化、高精度、高效率地实现制造设计，大大缩短产品开发周期。
- 动画设计：用户群主要是电视台、广告公司、影视制作公司、游戏软件开发公司、室内装饰公司，通过图形工作站强大的二维、三维图形图像计算处理能力，完成各种二、三维动画设计。
- GIS 地理信息系统：客户群主要是城市规划单位、环保部门、地理地质勘测院、研究所等，通过在图形工作站上运行的 GIS 软件，实现各类行业管理信息与空间地理信息的集成。
- 平面图像处理：用户通常是以图形工作站为硬件平台，以 Photoshop、CorelDraw 等软件为操作工具，致力于图片影像处理、广告及宣传彩页设计、包装设计、纺织品图案设计等。
- 模拟仿真：在军事领域，模拟仿真技术是训练战斗机驾驶员、坦克驾驶员以及模拟海上航行的有效手段；在科研开发领域，它使设计者在制作样机之前，就可以在图形工作站上进行仿真运行，及时发现问题，对设计进行修改。

典型的工作站包括一个 32 位高速微处理器，64 位浮点处理单元，Unix 操作系统/X Windows 图形用户界面，加速图形控制器，17～19 英寸彩色显示器和内置的以太网联网功能。

3．小型机

小型机是指运行原理类似于个人计算机，但性能及用途又截然不同的一种高性能计算机，它是 20 世纪 70 年代由 DEC（数字设备公司）公司首先开发的一种高性能计算产品。

小型机具有区别 PC 及其服务器的特有体系结构，同时应用了各制造厂自己的专利技术，有的还采用小型机专用处理器。例如美国 Sun、日本 Fujitsu（富士通）等公司的小型机是基于 SPARC 处理器架构，美国 HP 公司的小型机是基于 PA-RISC 架构。

小型机的 I/O 总线也不同于一般的个人计算机，例如 Fujitsu 是 PCI，Sun 是 SBUS。这同样意味着各公司小型机上的插卡，如网卡、显示卡、SCSI 卡等可能也是专用的。

此外，小型机使用的操作系统一般是基于 Unix 内核的专用产品，Sun、Fujitsu 使用的操作系统是 Sun Solaris，HP 小型机使用的是 HP-UX，IBM 小型机使用的是 AIX。

所以小型机是封闭专用的计算机系统，使用小型机的用户一般是看中 Unix 操作系统的安全性、可靠性和专用服务器的高速运算能力。

在网络工程中，如果用户对应用提出了较为苛刻的安全性、可靠性和专用性的要求，则可以考虑采用小型机作为应用的服务器。

4．中型机

在当前的网络工程中，已经不再严格划分中型机和小型机，更多的情况下，中型机更相当于小型机中的高档产品。

在大多数厂商的非 x86 服务器产品中，一般会存在着多种系列，最常见的产品划分方式为部门级服务器、企业级服务器和电信级服务器，大多数情况下，可以将部门级、企业级服务器等同于小型机，而将电信级服务器等同于中型机。

5. 大型机

大型机和相关的客户机-服务器产品可以管理大型网络，存储大量重要数据以及驱动数据并保证其数据的完整性。大型机系统具有较高的可用率、高带宽的输入输出设备、严格的数据备份和恢复机制、高水平的数据集成和安全性能。

大型机由 CPU、主存操作员控制台、I/O 通道、通信控制器、磁盘控制器、存储控制器、磁带子系统、显示器、打印机等组件构成，具有物理尺寸大、系统容量大、运行速度高、容错能力强、系统安全性高、事务处理能力强的特点。

大型机目前仍然在金融行业、记账系统、订单处理系统、大型互联网应用、复杂数据处理、联机交易系统、科学计算等领域发挥作用，但是随着计算机小型化的发展，大型机将逐步退出应用市场。

在网络设计中，只有全国、全行业级的应用中，才会出现大型机的应用需求。

6. 输出——计算机平台需求表

计算机平台需求表是总结用户对计算机平台需求的表格，通过对该表格的填写，为后期的计算机平台参数指标确定工作奠定基础。表 2-6 是各类计算机平台的需求表。

表 2-6 计算机平台需求表

指标分类	指标子项	指标要求
CPU	型号	
	时钟频率	
	前端总线频率	
	指令位数	
	CPI/IPC	
	CPU 个数	
内存	大小	
	访问延迟	
	容错	
Cache	一级容量	
	二级容量	
硬盘	数量	
	大小	
	转数	
	接口类型	

续表

指标分类	指标子项	指标要求
网络接口	传输速率	
	网卡数量	
	接口类型	
电源功耗	个数	
	功率	
	冗余	
物理指标	长度	
	宽度	
	高度	
	重量	
	…	

2.3.2.5　网络需求

需求分析的最后工作是考虑网络管理员的需求，这些需求包括以下内容：

- 局域网功能。
- 网络拓扑结构。
- 性能。
- 网络管理。
- 网络安全。
- 城域网/广域网的选择。

1. 局域网功能

1）局域网网段分布

传统局域网络中，由二层交换机构成局域网骨干，整个网络其实是一个广播域；在这样的网络中，网段是由交换机上的一个端口下连的共享设备形成的；网段内部用户间通信不需要通过交换设备，而段间通信需要通过交换设备进行存储转发。

在现代局域网中，由于三层交换技术的引入，由三层交换设备构成局域网骨干，这个网络中存在多个广播域，其实是多个小型局域网，这些小型局域网通过三层设备的路由交换功能互联；在这种局域网络中，网段的概念发生了变化，其实就是一个独立的广播域，一个典型的 VLAN。

无论是哪种网段，都是计算机节点的一种划分方式，但是基于三层交换技术的网段划分方式逐渐成为主流；一般情况下，局域网网段和用户群的分布是一致的，但是也存在一定的差异；允许一个网段内部存在多个用户群，也允许一个用户群占据多个网段。

对于升级的网络，可以对现有网段划分方式进行改进，形成新的划分方案；对于新建网络，则是和网络管理员一起商量网段划分方式；无论哪种情况，最终都应形成网段分布需求，也就是用户群和网段的关系需求。

2）评估局域网网段

局域网网段的分布，主要是依据业务上的特殊要求，而这些业务上的特殊要求，会导致不同的网段存在不同的功能要求。在进行网络需求收集时，应该找到各网段所需要的功能清单，并明确网段中功能的重要性。表 2-7 是一个局域网功能表示例，借助于该功能表，可以方便地进行各网段的网络功能收集工作。

表 2-7　局域网功能表

网段分布 / 功能	服务器网段 (1~100)	管理网段 (1~100)	X 网段 (1~100)	Y 网段 (1~100)	Z 网段 (1~100)
文件服务					
E-mail 服务					
打印服务					
数据库服务					
应用服务					
网络传真服务					
P2P 应用服务					
视频服务					
系统管理服务					
网络管理服务					
安全管理服务					
数据备份服务					
其他服务					
…					

（注：网段的百分率可以通过用户数的比例来产生。）

3）局域网负载

局域网的负载是和应用有关联的，根据局域网络的功能需求，可以分析出局域网络的负载。在进行网络负载分析时，要针对各种应用和功能服务，评估服务的平均事务量或文件传输大小，同时估算用户访问频率，经过简单计算就可以估算出网络的负载。

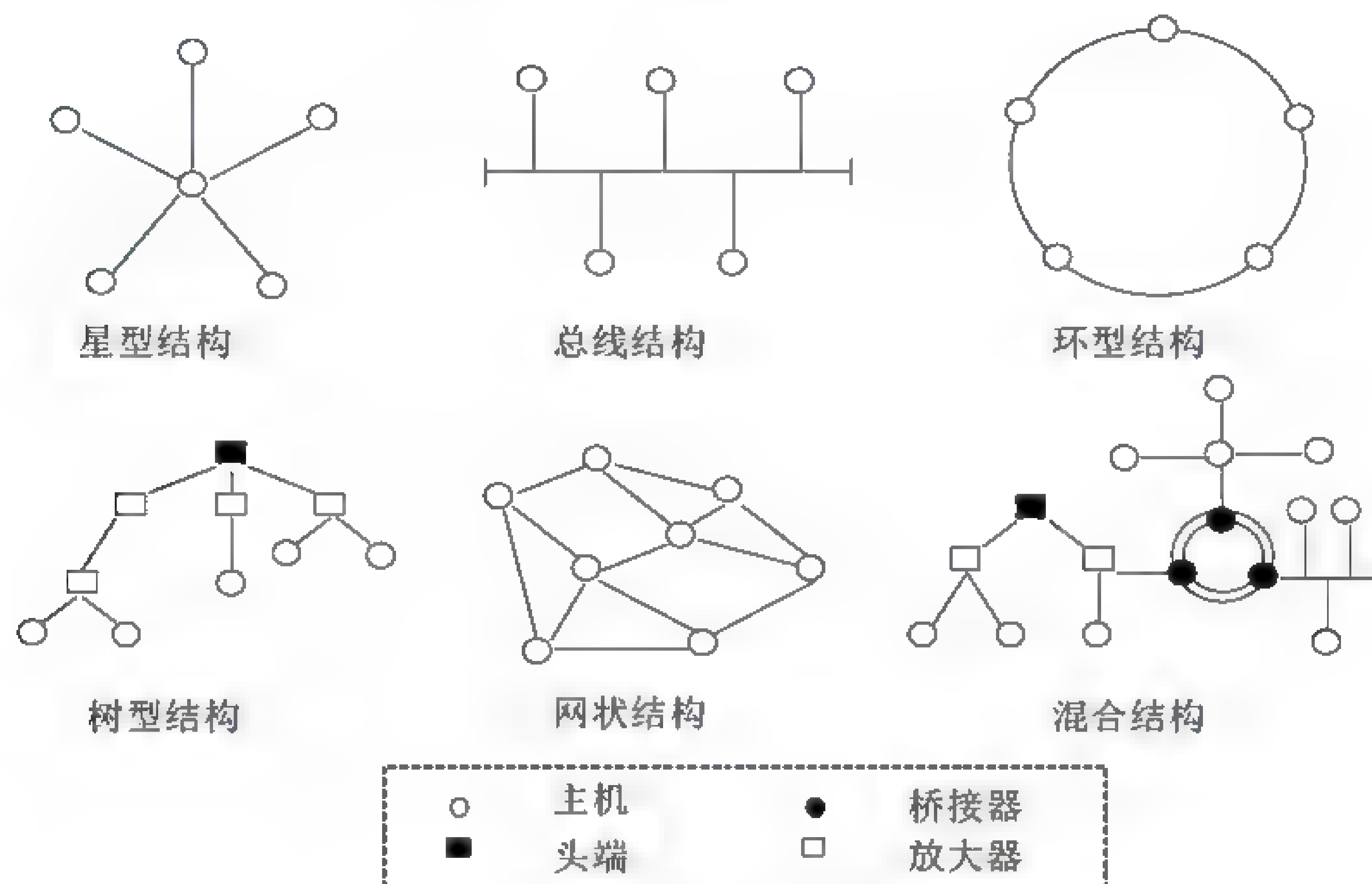
对于升级的网络，可以对现有网络通过各种测试工具获取网络流量分析，从而获取当前网络的负载，作为升级后网络负载的参照。

对于非专用设计标准，根据经验或简单的方法进行评估就可以了；对于较为复杂、网络要求较高的网络，对各种服务的平均事务量、文件传输大小、用户访问频率，都应根据实际测试的值，来进行局域网的负载运算。

2．网络拓扑结构

网络拓扑结构分为广域网拓扑结构和局域网拓扑结构，这两类拓扑结构的差异性较大。

局域网的一个重要特征就是在信息传输上采用广播方式，其覆盖范围小、专用性强，具有较为稳定和规范的拓扑结构。传统局域网中常见的网络拓扑结构包括星型结构、总线型结构、树型结构、环形结构等，图 2-19 为局域网拓扑结构的示意图。在现代交换网络中，部分传统拓扑结构已经不再沿用，但星型结构、环型结构等拓扑结构仍在发挥作用。



2-19　局域网拓扑结构

广域网在信息传输上采用点到点方式，其连接主要依靠公用通信设施，网络拓扑结构较为复杂。传统广域网拓扑结构主要包括集中式拓扑结构、分散式拓扑结构、分布式拓扑结构等，图 2-20 为广域网拓扑结构的示意图。在现代网络中，这些拓扑结构仍在大量使用。

在收集网络需求时，需要和网络管理人员就网络拓扑结构进行讨论，并就网络拓扑结构的优劣进行分析，然后达成一致性意见。

3. 性能

网络需求收集工作中，针对网络的性能需求，可以考虑以下方面内容：

- 网络容量和响应时间。
- 可用性。
- 备份管理和存档。

网络的性能需求是在需求分析过程中，由网络管理人员提出的，这些需求不同于用户需求和应用需求，它来自于网络管理人员的工程和管理经验。这些性能需求不能作为设计工作的直接依据，但是应作为参考要求。

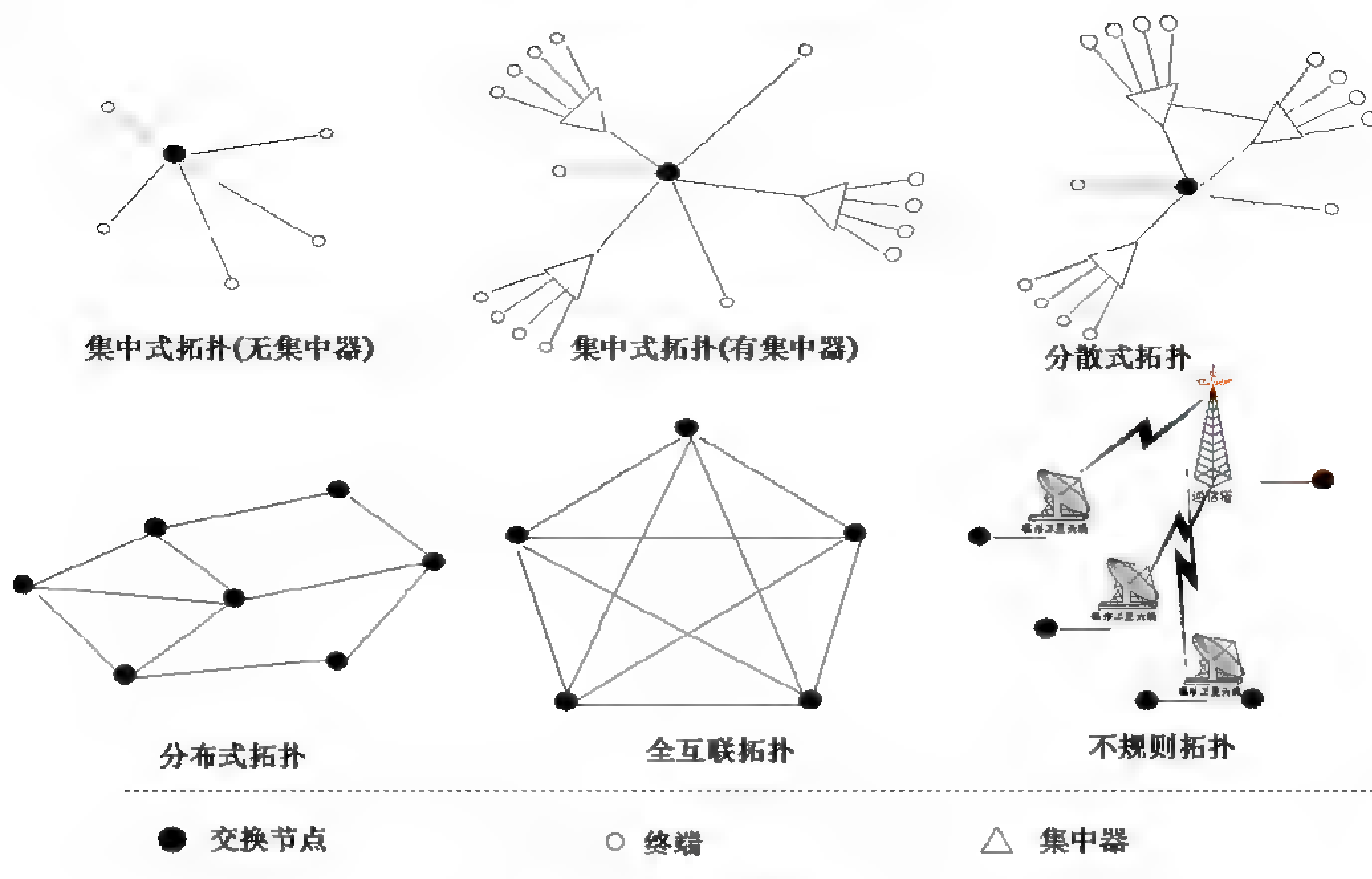


图 2-20　广域网拓扑结构

1）网络容量和响应时间

这里的网络容量和响应时间要求，并不是来自于复杂的网络分析，而是直接来自于网络管理人员的要求。在有些网络工程中，网络管理人员提出的网络容量和响应时间要高于用户和应用的需求。

2）有效性

有效性需求是指在进行网络建设策略的选择时产生的各种过滤条件，不满足条件的策略是不能被选择的。有效性条件没有固定的模式，主要是由各种条件构成，通常考虑如下方面的内容。

- 局域网拓扑结构：网络管理人员认同的拓扑选择条件会对后期的设计产生影响，例如不能存在单点效应等。
- 网络设备：网络管理人员提出的各种网络设备选择条件，甚至是网络管理部门认同的产品喜好等，会直接决定能够采购的网络产品范围，例如核心设备不选择国产设备、网络设备要采用标准协议等。
- 服务器设备：由于服务器产品较为统一，因此选择条件相对较为统一，例如 PC 服务器不选择塔式服务器，服务器选择两路 CPU 还是四路 CPU 等。
- 存储设备：存储设备由于其特殊性，选择性条件较多，并且直接关系到产品的选

型，例如存储产品是否和服务器产品的厂商保持一致，是采用 FC-SAN 还是采用 IP-SAN，带库是采用物理带库还是虚拟带库等。

- 安全设备：安全设备种类繁多，设计复杂，虽然形成了特定的安全体系，但是仍缺乏统一的标准，因此安全设备选择条件较为复杂，例如安全产品能否选择国外产品，是否考虑物理安全技术，是否实现防火墙和 IDS 联动等。
- 机房：机房选择条件非常复杂，从装饰材料的选择到门禁系统的要求等，涵盖了机房装修的各个方面。
- 产品供应商的选择条件：产品供应商的选择条件，主要是针对产品供应、备品备件、厂商服务等提出的明确要求，这些是选择产品供应商的关键。
- 线路运营商的选择条件：网络管理人员一般会针对线路运营商提出较为明确的选择条件，包括维护人员要求、线路冗余要求、故障响应要求、代维要求等。
- 集成商的选择条件：集成商选择条件将直接决定入围的集成商，一般包括注册资金、流动资金、人员数量、高级工程师数量、集成资质等内容。

在网络设计工作中，这些琐碎的选择条件，其实对设计工作的影响是非常大，很多项目就是因为在需求调查工作中，没有注意这些有效性条件的收集而导致了失误和失败。

3）数据备份和容灾需求

数据备份和容灾需求是网络工程中的重点内容，对于一些特定行业来说，数据是至关重要的，数据一旦丢失，将会造成不可挽回的损失。因此，对数据备份和容灾需求是网络需求调查中的重点内容。

根据不同的网络工程规模，存在两种建设情况，一种是需要建设复杂的数据中心和容灾备份中心，另外一种仅建立数据备份和容灾机制。

（1）数据中心和容灾备份中心。

数据中心建设需要收集的需求包括以下一些内容：

- 链路和带宽需求。
- 接入设备需求。
- 互联协议需求。
- 数据中心局域网区域划分需求。
- 数据中心设备需求。
- 数据库平台需求。
- 安全设备需求。
- 机房及电源需求。
- 数据中心托管及服务需求。
- 数据资源建设规划需求。
- 数据备份管理机制需求。

容灾备份中心的需求内容和数据中心基本一致，但是建设内容稍有差异。

在数据中心和容灾备份中心之间关键的是容灾方式，容灾方式的建设分为数据级容灾和应用级容灾，并且容灾方式存在国际标准，应正确引导网络管理人员，达成数据中心、容灾备份中心、容灾方式建设需求的一致性。

（2）数据备份和容灾机制。

相对于建设复杂的数据中心和容灾备份中心这样庞大的工程，建立简单有效的数据备份和容灾机制，对小型网络是合适并有效的。

正确备份信息在网络恢复信息时显得尤为重要，必须制订很好的防御和恢复策略，必须执行严格的备份过程和存档处理。在选择备份方针和技术时，必须对整个组织的风险做一下评估，确定各种数据的相对重要性。

制订的恢复方案至少应该包括如下内容：

- 选择媒体以供备份，包括磁盘阵列或者磁带库。
- 保护现场数据。
- 保护现场外的备份数据。
- 制定数据应急预案。

4．网络管理

网络管理人员的管理思路、产品喜好、管理要求是决定建设网络管理平台的关键，由于网络管理是网络工程中较为复杂，牵涉面较广的建设内容，需要与网络管理人员重点进行交流，获取明确的需求。网络管理的需求主要从以下方面进行。

1）建设思路及目的

- 明确网络管理的目的。企业网络管理的主要目的是提高网络可用性、改进网络性能、减少和控制网络费用以及增强网络安全性等，网管员可以根据自身需要进行补充与调整。
- 掌握网络管理的要素。网络管理平台的建设要注意与企业业务需求的结合，完整而理想的网络管理解决方案，应该根据应用环境和网络对业务流程，以及用户需求的端到端关联关系，来管理网络及其所有设备。
- 明晰管理的网络资源。网络资源就是指网络中的硬件设备、整个环境中运行的软件以及所提供的服务等，网络管理员必须明确需要管理的资源。
- 注重软件资源管理和软件分发。网络管理系统的软件资源管理和软件分发功能，是指优化管理信息的收集，此外软件资源管理是对企业所拥有的软件授权数量和安装地点进行管理。软件分发则是通过网络把新软件分发到各个站点，并完成安装和配置工作。这些特定的需求需要管理员进行明确。
- 应用管理不容忽视。应用管理用于测量和监督特定的应用软件及其对网络传输流量的影响。网络管理员通过应用管理可以跟踪网络用户和运行的应用软件，改善网络的响应时间。网络管理人员应明确在应用管理方面的需求。

2）网络管理功能要求

网络管理具有五大基本功能，设计人员应协助网络管理员对各种功能提出较为明确的需求。

- 性能管理：管理员要明确性能管理的内容，主要是需要监视网络运行的参数，如吞吐率、响应时间、网络的可用性等。
- 故障管理：管理员要明确故障的展现形式、记录方式、应急响应机制等要求。
- 配置管理：管理员要明确配置管理的图形展现要求、设备配置要求、设备状态配置要求等基本需求。
- 计费管理：管理员要明确计费方式、费用数据采集等基本需求。
- 安全管理：网管系统对安全管理的功能较弱，管理员要明确安全管理的具体内容。

3）网络管理软件

选择网管软件的要求直接体现了网管人员的产品喜好，同时也可以明确对网管软件的要求。

- 企业需要哪些管理功能：网管软件都是价格不菲的，所以在为企业选择网管软件时，一定要考虑到目前与未来企业网络环境发展的需要。一个好的网络管理系统必须适合企业业务发展的需要。
- 网络管理软件支持哪些标准：网管人员需要明确产品对网管协议的支持程度，尤其是 SNMP 和 RMON 协议，需要明确到协议的版本和关键细节。
- 支持各种硬件、软件的范围：不同网管软件对不同产品的支持是不一样的，管理人员需要明确什么样的硬件、软件纳入网络管理范畴，才能设定符合要求的产品范围。
- 可管理性：可管理性是由网管需求对被管理设备提出的需求，可管理性要求指设备对协议、管理信息库等、图形库等各方面的支持，也属于网管平台的需求。

5．网络安全

网络安全体系是建设网络工程的有效内容之一，不管网络工程规模如何，都应该存在一个可扩展的总体安全体系框架。对于不同的网络工程，允许建设不同的安全体系框架，图 2-21 就是一个较为常见、可行的安全体系框架，设计人员在进行网络安全需求收集时，可以依据该框架进行安全需求的明确。

在图 2-21 所示的安全体系框架中，安全管理体系是整个安全架构的基础，使安全问题可控可管；以安全技术为核心的技术措施（包括机房及物理线路安全、网络安全、系统安全、应用安全、安全信任体系等），使安全手段更加可靠；以容灾与恢复为目标的后备保障措施，可以对付重大灾难性事件后的网络重建；以安全运维支持服务作为外部支撑条件，使安全问题能够及时有效地解决。

基于以上框架，对于网络安全的需求，设计人员应该协助网络管理人员，对安全管理体系、运营服务体系、数据容灾与恢复、安全信任体系等方面的需求进行确定。同时，对于技术措施需求，可以借鉴表 2-8 的内容进行明确。



图 2-21 安全体系框架的示例

表 2-8 技术措施需求表

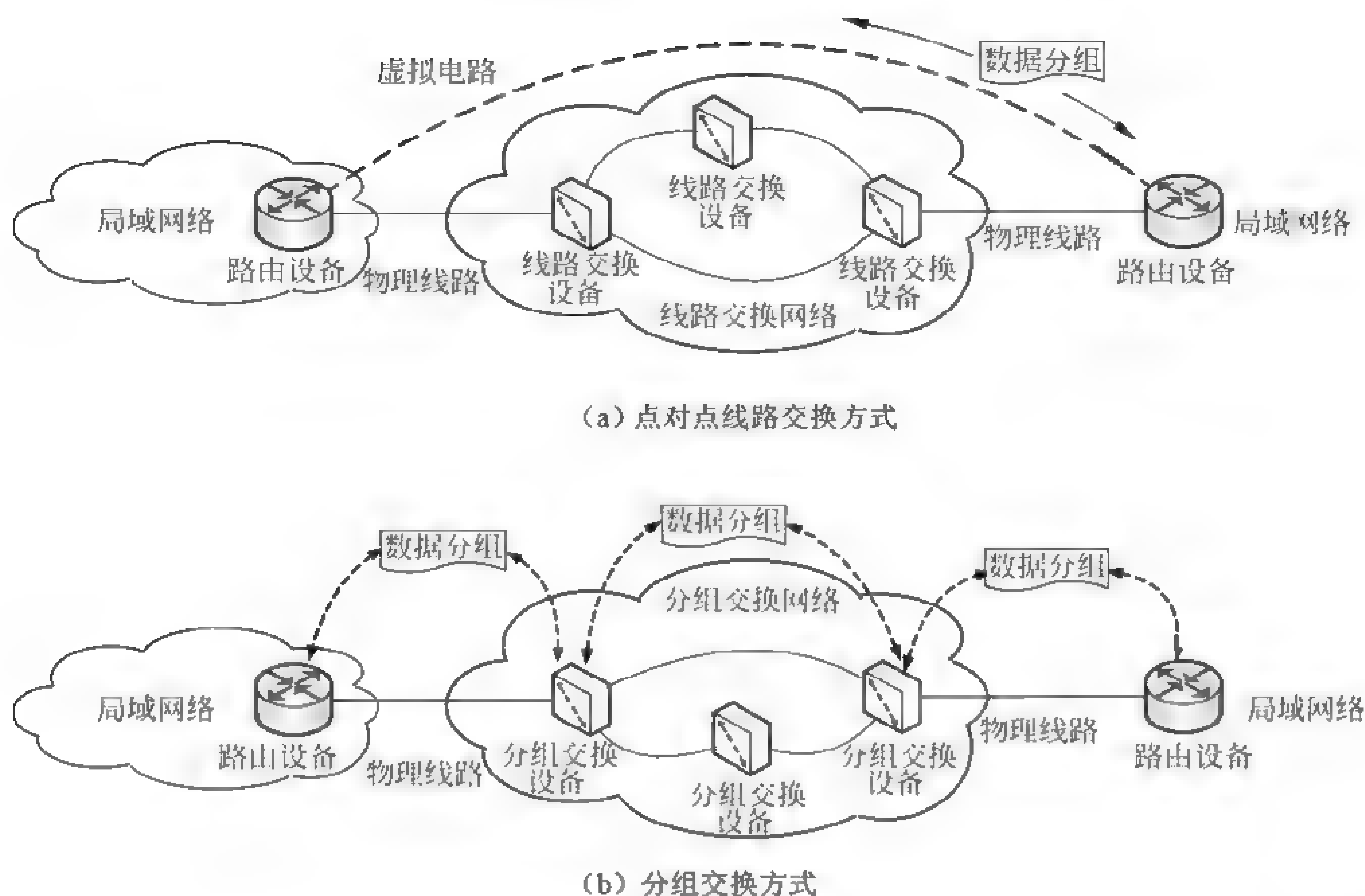
技术措施层次	需求项目	需求项目	需求项目	需求项目
机房及物理线路安全需求	机房安全	计算机通信线路安全	骨干线路冗余防护	主要设备的防雷击措施
网络安全需求	安全区域划分	安全区域级别	区域内部安全策略	区域边界安全策略
	路由设备安全	网闸	防火墙	入侵检测
	抗 DDoS	VPN	流量管理	网络监控与审计
	网络监控与审计	访问控制		
系统安全需求	身份认证	账户管理	主机系统配置管理	漏洞发现与补丁管理
	内核加固	病毒防护	桌面安全管理	系统备份与恢复
	系统监控与审计	访问控制		
应用安全需求	数据库安全	邮件服务安全	Web 服务安全	应用系统定制安全

6. 城域网/广域网的选择

对于一般的网络工程来说，城域网和广域网用于连接局域网，并形成完整的企业网络或者行业网络。城域网/广域网通过连接设备和通信线路，实现各远程局域网络之间的互联，而选择通信线路实现连接则是建设城域网/广域网的重点。

选择城域网/广域网可供选用的连接方案有以下两种，如图 2-22 所示。

- 点对点线路交换服务（拨号线路或租用线路）。
- 分组交换服务。



（a）点对点线路交换方式

（b）分组交换方式

图 2-22　城域网/广域网连接方案

如图 2-22 所示，在点对点线路交换服务方式中，存在局域网路由设备和线路交换设备两类设备，这些设备之间通过物理线路互连，在路由设备之间建立的是虚拟电路，数据分组仅在路由设备上进形封装和解封，在线路交换设备以数据帧或信号的方式进行传递；在分组交换方式中，路由器和分组交换设备之间通过分组交换协议互连，数据分组在路由设备、分组交换设备上都存在封装和解封。所以，点对点线路交换方式中，相当于两台局域网路由器通过虚拟电路直接互连，而分组交换方式中，两台局域网路由器之间存在由多个路由设备构成的分组网络。

1）点对点线路交换服务

点对点连接是在两个节点间建立一个永久的或暂时的虚拟或物理连接。较为常见的点对点服务如表 2-9 所示。

表 2-9　常见点对点线路交换服务

技 术 类 型	数据传输率	物 理 介 质	备　　注
拨号线路	14.4～56Kbps	双绞线	音频线路
卫星	400～2Mbps	双绞线	微波线路
T1	1.544Mbps	无线电波	同步时分复用线路
E1	2.048Mbps	双绞线、光纤	同步时分复用线路

续表

技 术 类 型	数据传输率	物 理 介 质	备 注
T3	45Mbps	同轴电缆	同步时分复用线路
OC-3	155.52Mbps	光纤	异步时分复用线路
OC-12	622.08Mbps	光纤	异步时分复用线路
OC-48	2.488Gbps	光纤	异步时分复用线路
OC-96	9.953Gbps	光纤	异步时分复用线路
SDH STM-1	155.52Mbps	光纤	同步时分复用线路
SDH STM-4	622.08Mbps	光纤	同步时分复用线路
SDH STM-16	2.488Gbps	光纤	同步时分复用线路
SDH STM-64	9.953Gbps	光纤	同步时分复用线路

2）分组交换服务

分组交换服务在连接广域网节点时灵活性更大，并且成本较低；随着运营商在数据网络上的投入逐步增加和 VPN 技术的发展，通过包交换服务来连接局域网络已经成为主流方式。表 2-10 列出了常见的分组交换服务方式。

表 2-10 常见分组交换服务

技术类型	数据传输率	物 理 介 质	备 注
X.25	64Kbps	同轴电缆	数据分组交换，IP 为网络层常见协议
ISDN	128Kbps～1.544Mbps	双绞线	数据分组交换，IP 为网络层常见协议
帧中继	64Kbps～1.544Mbps	双绞线	数据帧交换，IP 为网络层常见协议
ATM	51.84Mbps～2.488Gbps	光纤	信元交换，IP 为网络层常见协议
以太网络	10Mbps～10Gbps	双绞线或光纤	数据帧交换，IP 为网络层常见协议
VPN	2Mbps～10Gbps	双绞线或光纤	IP 分组交换，借助于二层、三层隧道技术
MPLS VPN	2Mbps～10Gbps	双绞线或光纤	IP 分组交换，借助于 MPLS VPN 技术

7. 需求表

网络需求输出的表包括局域网功能、网络拓扑结构、网络管理、网络安全、城域网/广域网选择等分项需求表。由于网络需求涉及面广、内容较为复杂，而且不同的网络工程其网络需求差异较大，因此网络需求表并不需要严格的格式，设计人员可以根据上文内容，自行设计网络需求表格。

2.3.3 编制需求说明书

通过需求收集工作，网络设计人员会获取大量的需求信息，这些信息由各种独立的表格、散乱的文字以及部分统计数据等构成，这些需求信息应整合形成正式的需求说明书，以便于后期设计、实施、维护工作的开展。

需求说明书是网络设计过程中第一个正式的可以传阅的重要文件，其目的在于对收集到的需求信息作清晰的概括整理，这也是用户管理层将正式批阅的第一个文件。

1．数据准备

数据准备工作是开始编制需求说明书的前期工作，主要由两个步骤构成：

第一步是要将原始数据制成表，从各个表看其内在的联系及模式；

第二步是要把大量的手写调查问卷或表格信息转换成电子表格或数据库，由于录入工作量较大，可以求助于用户单位或雇用临时工。

另外，对于需求收集阶段产生的各种资料，包括手册、报表、原始单据等，无论其介质是纸质还是电子的，都应该编辑目录并归档，便于后期查阅。

2．需求说明书的组成

编写需求说明书的目的是能够向管理人员提供决策用的信息，因此说明书应该做到尽量简明且信息充分，以节省管理人员的时间。

网络需求说明书不存在国际或国家标准，即使存在一些行业标准，也只是规定了需求说明书的大致内容要求。这主要是由于网络工程需求涉及内容较广，个性化较强，而且不同的设计队伍对需求的组织形式也不一样。

对网络需求说明书，存在两点要求：首先，无论需求说明书的组织形式如何，网络需求说明书应包含业务、用户、应用、计算机平台、网络 5 个方面的需求内容；其次，为了规范需求说明书的编制，一般情况下，需求说明书应该包括以下 5 个部分：

- 综述。
- 需求分析阶段概述。
- 需求数据总结。
- 按优先级排队的需求清单。
- 申请批准部分。

3．综述

需求说明书的第一部分内容是综述，对网络工程项目的主要内容、重要性等进行一个简单的描述。综述应包括的内容如下：

- 对项目的简单概述。
- 设计过程中各个阶段的清单。
- 项目各个阶段的状态，包括已完成的阶段和现在正进行的阶段。

4．需求分析阶段总结

需求分析阶段总结主要是总结需求分析阶段的工作，总结内容包括：

- 接触过的群体和代表人名单。
- 标明收集信息的方法（访谈、集中访谈、调查等）。
- 访谈、调查总次数。
- 取得的原始资料数量（调查问卷、报表等）。

- 在调查工作中遇到的各种困难等。

5．需求数据总结

对从需求调查中获取的数据，需要认真总结并归纳出信息，并通过多种形式进行展现。在对需求数据进行总结时，应注意以下几点。

（1）简单直接。提供的总结信息应该简单易懂，并且将重点放在信息的整体框架上，而不是具体的需求细节。另外，为了方便用户进行阅读，应尽量使用用户的行业术语，而不是技术术语。

（2）说明来源和优先级。对于需求，要按照业务、用户、应用、计算机平台、网络等进行分类，并明确各类需求的具体来源（例如人员、政策等）。

（3）尽量多用图片。图片的使用可以使读者更容易了解数据模式，在需求数据总结中大量使用图片，尤其是数据表格的图形化展示，是非常有必要的。

（4）指出矛盾的需求。在需求中会存在一些矛盾，需求说明中应对这些矛盾进行说明，以使设计人员找到解决方法；同时，如果用户人员给出了矛盾中目标的优先级别，则需要特殊标记，以便在无法避免矛盾的时候，先实现高级别的目标。

6．按优先级排队的需求清单

对需求数据进行整理总结之后，按照需求数据的重要性列出数据的优先级别清单。

7．申请批准部分

在编写需求说明书时，需要预留大量对需求进行确认或者申请批准的内容，确切地说，就是要预留大量用户管理人员签字的空间。由于需求说明书是开展后期设计工作的基础，必须避免用户需求和收集材料的不一致性，因此预留申请批准部分是必需的。

8．修改需求说明书

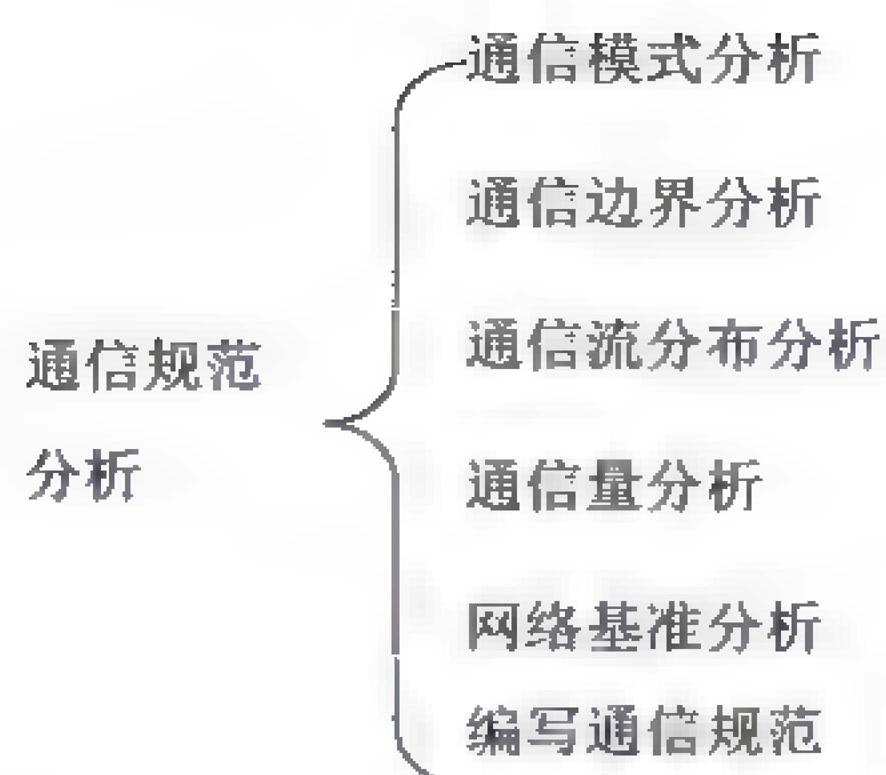
由于需求经常发生变化，因此，在编写需求说明书的时候，也要考虑到怎样设计修改需求说明书。如果的确需要修改，最好不要改变原来的数据和信息，可以考虑在需求说明书中附加一部分内容，说明修改的原因，解释管理层的决定，然后给出最终的需求说明。

2.4 通信规范

2.4.1 通信规范分析

在网络的分析和设计过程中，通信规范分析处于第二个阶段，通过分析网络通信流量和通信模式，发现可能导致网络运行瓶颈的关键技术点，从而在设计工作避免这种情况的发生。

通信规范分析通过对通信流量的大小和通信模式的估测和分析，为逻辑设计阶段提供了重要的设计依据。由于网络的复杂性，通信规范分析的成果必然允许存在一定误差，但是这些成果依然可以为设计工作带来很大的便利，避免设计工作的盲目性。



2.4.2　通信模式

在计算机网络中，通信是通信模式和通信量的组合。在第 2.3.2 节介绍应用需求时，提到了应用软件按照网络处理模型，可分为单机软件、对等网络软件、C/S 软件、BPS 软件、分布式软件，而这些应用的网络处理模式对于网络设计来说，其数据的网络传递模式就是通信模式。在通信规范分析阶段，了解通信模式非常重要，该通信模式将直接决定网络流量在不同网段的分布，同时结合流量的通信量，就可以获取不同网段的总通信量大小。

通信模式基本与应用软件的网络处理模型相同，也分为 4 种：

- 对等通信模式。
- 客户机-服务器通信模式。
- 浏览器-服务器通信模式。
- 分布式计算通信模式。

网络中每个网络节点工作在何种模式下，主要取决于网络资源、节点和应用程序的分布，大多数时候，网络节点会同时工作在多种模式下。例如，一台工作站既需要和同工作组的计算机进行对等通信，同时，由于安装了 C/S 软件，又需要和服务器进行通信。

由这 4 种通信模式分析得到的通信规范可以使设计者对网络的分析设计工作有一个全面的了解；同时，对确定网络的逻辑网络设计和物理网络设计起着重要的作用。此外，在逻辑网络设计阶段，通信模式还可以帮助网络设计者了解网络的性能特性和互联策略。

1．对等通信模式

对等通信模式指相似计算机节点间的通信，在这种模式中，参与的网络节点都是平等角色，既是服务的提供者，也是服务的享受者。由于参与通信的节点有相似的应用程序和通信能力，因此在对等通信模式中，流量通常是双向对称的。对等通信模式的最大用途在于在局域网段中，计算机都被配置成为对等方式，不需要借助于中心服务器来完成通信；另外，随着 QQ、BT、视频会议等基于互联网的 P2P 应用的推广，对等通信模式开始突破局域网络，并开始对网络产生巨大的影响。

典型的对等通信模式包括以下内容：

- 利用 P2P 协议的 BT、超级旋风等软件，这些软件在运行时，既从网络上获取文件数据块，同时也提供已下载文件块的共享，所有节点既是服务器也是客户机。
- 处于远程站点的商业人员之间使用视频会议系统召开会议是对等通信应用的一个例子。在会议过程中，每个与会人员都可以随时按其所需来交流，所有站点对服务质量的需求都相同。

在对等通信模式中，每个节点都有可能与网络中的其他节点建立连接或者发送数据，但是在进行通信规范分析时，可以认为对于每个节点来说，都抽象成一个双向的输入输出流，该流的输入和输出流量一致，如图 2-23 所示。

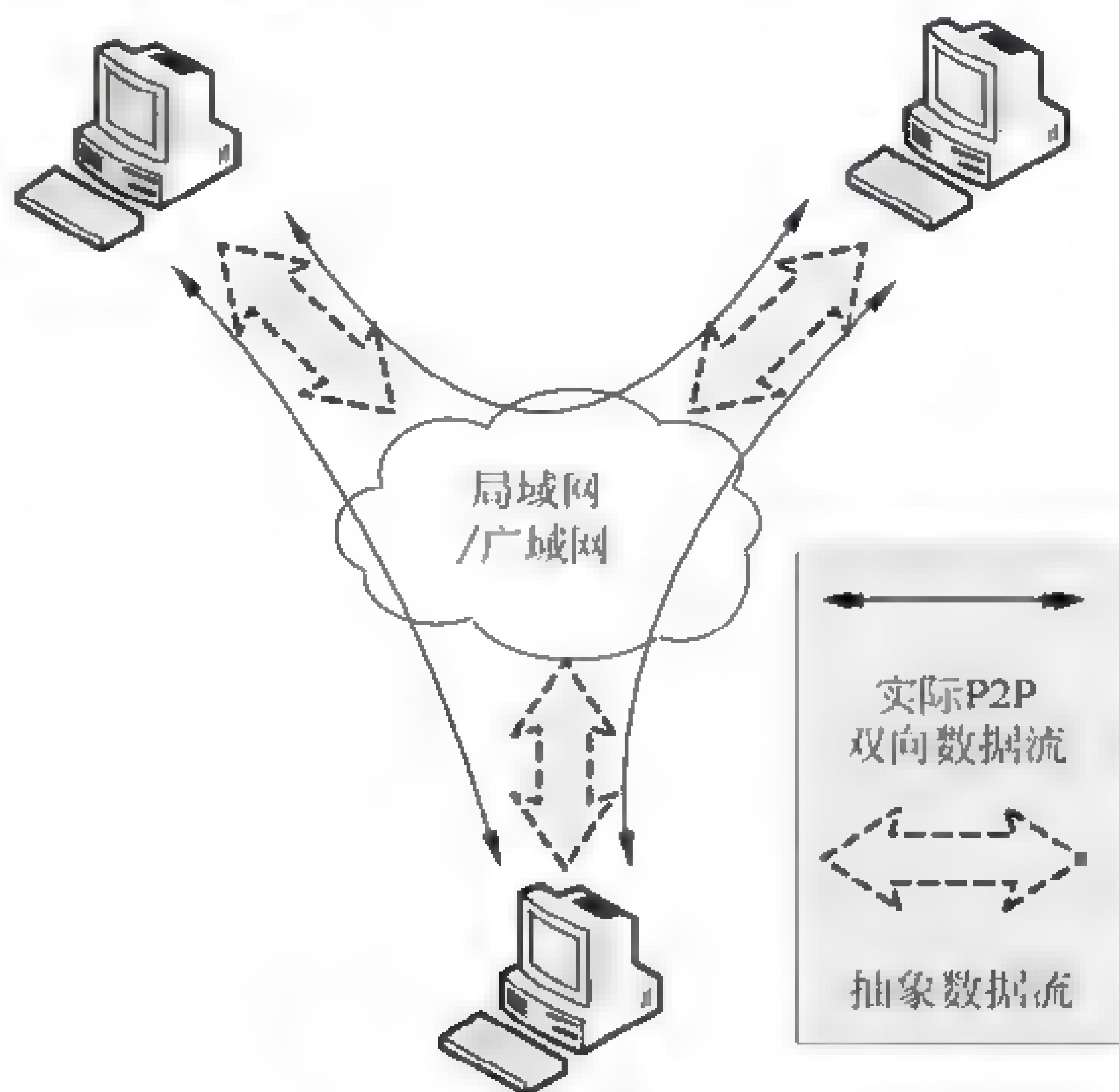


图 2-23 对等通信模式

2．客户机-服务器通信模式

客户机-服务器通信模式（Client/Server，C/S）是指在网络中存在一个服务器和多个客户机，由服务器负责进行应用计算、客户机进行用户交互的通信模式，也是目前应用最为广泛的一种通信方式。

客户机-服务器通信模式对客户机、服务器的选型并没有严格限制，应根据应用需要进行选择；与对等通信的随机模式不同的是，客户机-服务器通信模式有其方向性，通信流向取决于各个客户机使用的应用程序类型。图 2-24 是客户机-服务器通信模式中的网络流量分布。

在客户机-服务器通信模式中，信息流量以双向非对称的方式流动，因此可以分解成客户机至服务器和服务器至客户机两个信息流向，在不同的应用中，这两个流向的通信

流量是不同的，所以要分开进行计算。

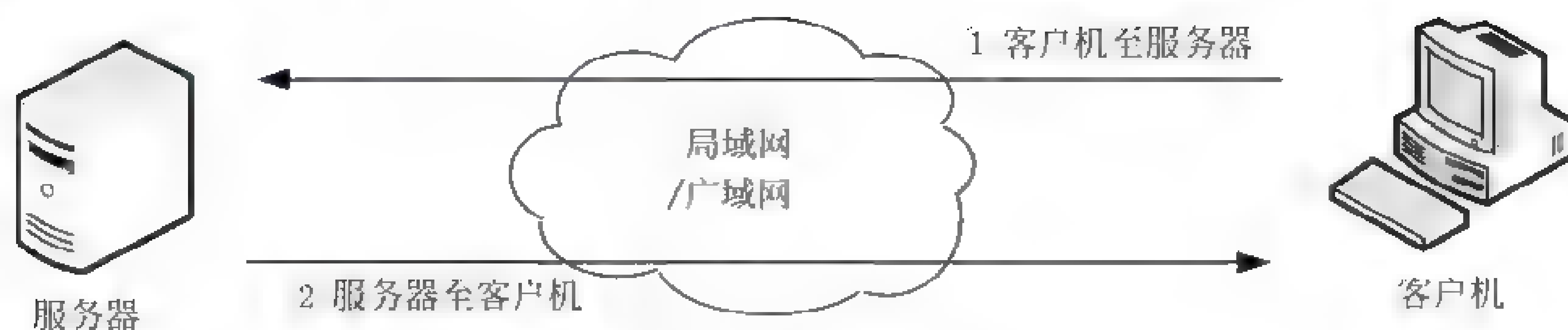


图 2-24 客户机-服务器通信模式

（1）服务器至客户机流量大。

在视频点播服务中，所有的客户机通过安装的视频点播软件访问服务器上的视频资源，客户端软件仅仅向服务器提交格式简单、数据量较小的控制报文，而服务器端则需要以视频流的格式，以每秒 1～2Mbps 的速率向客户端发送数据；在视频点播服务中，客户机至服务器端的流量要远小于服务器至客户机的流量，甚至可以忽略不计。

这样的服务主要是多媒体类型服务，通常情况下客户端至服务器端的流量远小于服务器至客户端的流量，可以在进行通信规范设计时忽略不计。

另外，基于 HTTP 协议的 WWW 服务、OLAP 等服务，也属于这种情况。

（2）客户机至服务器流量大。

客户机至服务器流量比较大的应用较少，典型的是基于 SNMP 协议的网管服务，对于网管平台来说，各个被管理的设备都是客户端，而网管服务器则是服务器；网络设备不断向网管服务器发送大量的状态数据，而服务器仅返回应答或修改指令；因此客户机至服务器的流量要明显大于反向的流量。

这样的服务主要是监控、日志等类型的服务，在进行通信规范设计时，可以对服务器至客户机的流量进行忽略。

（3）双向流量大。

对于 C/S 通信模式，大多数应用双向的流量都比较大，双向的流量都和用户类型、服务时段、用户操作等因素有关。

例如，在邮件服务中，客户端借助于 SMTP 完成向邮件服务器发送大数据量的电子邮件，也可以通过 POP3 协议从邮件服务器上获取大数据量的电子邮件；在文件传输服务中，客户端既可以借助于 FTP 协议向文件服务器上载文件，也可以借助于同样的协议下载文件；在数据库服务器中，客户端既要向数据库服务器插入数据，也要完成数据的检索。

在这种类型的通信模式中，双向流量的大小关系并不严格地存在，而是根据用户使用情况决定的，因此在进行通信规范设计时，这类服务的双向流量都不能被忽略，应根

据应用的情况评估流量的大小。

3．浏览器-服务器通信模式

浏览器-服务器通信模式是三层模式与四层模式的典型代表，其表现是通过客户端的浏览器，应用服务器负责业务逻辑，数据库服务器完成数据存储、计算、处理和检索。浏览器-服务器通信模式中，存在应用服务器和多个客户机之间的通信以及应用服务器和数据库服务器之间的通信，如图 2-25 所示。

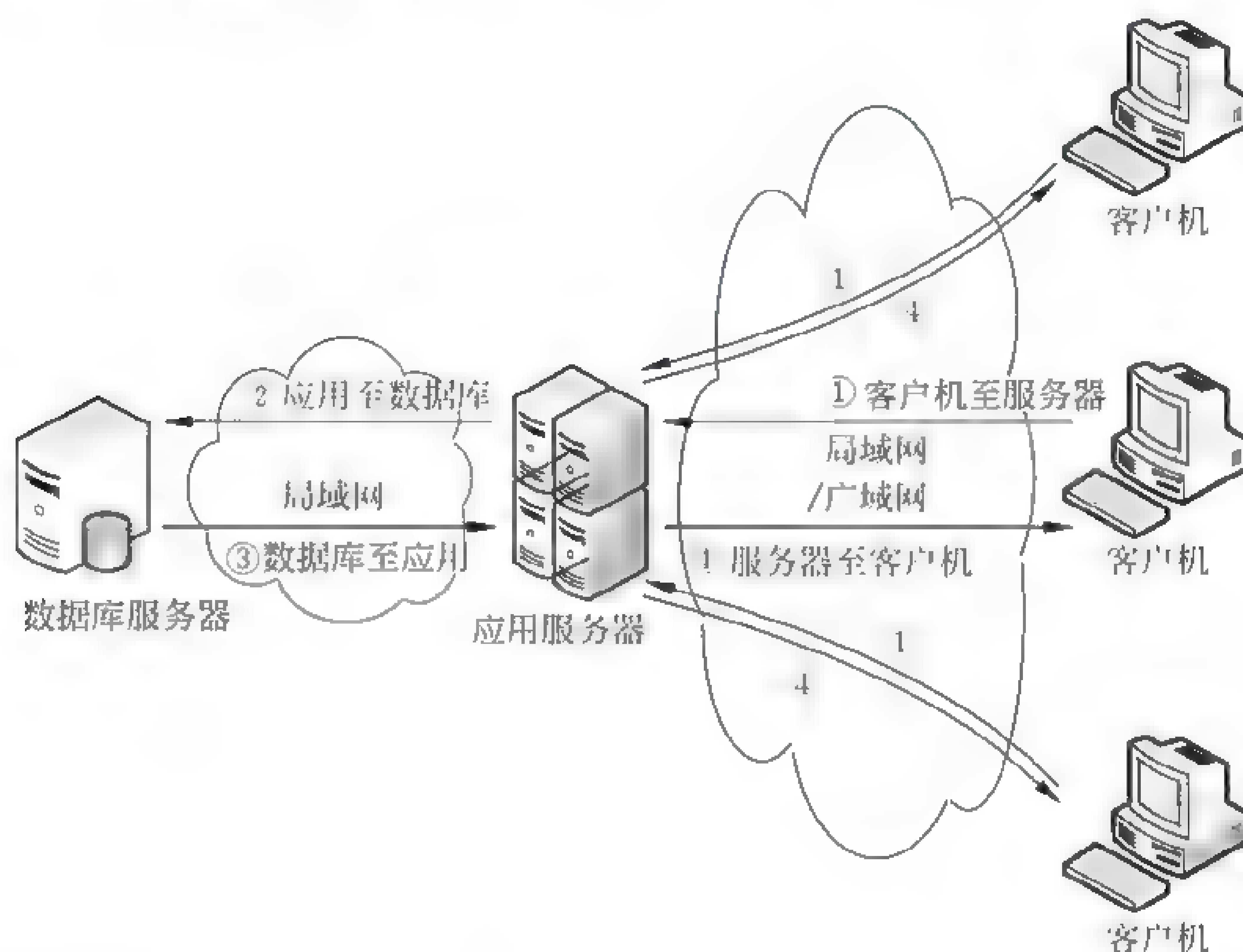


图 2-25　浏览器-服务器通信模式

浏览器-服务器通信模式较为特殊，可以将应用服务器与客户机之间的通信看成是一个典型的 C/S 通信模式，而将应用服务器与数据库服务器之间的通信看成是一个只有一台客户机（应用服务器被看成客户机）的 C/S 通信模式。应用服务器与客户机之间的通信，一般情况下属于“服务器至客户机流量大”的类型；而应用服务器与数据库之间的通信，一般属于“双向流量大”的类型。

4．分布式计算通信模式

分布式计算是指多个计算节点协同工作来完成一项共同任务的应用，在解决分布式应用，提高性能价格比，提供共享资源的实用性、容错性以及可伸缩性方面有着巨大的发展潜力。

分布式计算的通信流量特征比较复杂，一般情况下系统中存在少量任务管理节点和大量计算节点。对于有些系统来说，任务管理节点很少明确告诉计算节点应当做什么，

因此通信流量很少；而有些系统的任务管理节点及计算节点却很繁忙。由于任务管理节点根据当前资源的可用性及特定的资源分配策略分配任务，这使得通信流量难以预测。

2.4.3　通信边界

网络设计者必须清楚网络中的各种通信边界，这些边界当前主要以三种形式存在：一种是局域网络中的通信边界，一种是广域网络中的通信边界，另一种是虚拟专用网络的通信边界。

在网络设计中，通过对通信边界的分析，可以有助于设计人员找出网络中的关键点，因为通常情况下，通信的边界都是故障易发位置。

1. 局域网通信边界

局域网的通信边界主要是网络中的冲突域和广播域，在局域网络建设中，主要是通过划分冲突域和广播域来限制通信量。

1）冲突域和广播域

在传统的局域网络中，所有的计算机通过共享性连接设备进行互连。例如传统以太网络中，主要是通过同轴电缆、双绞线连接的中继器、集线器等设备构成局域网络。网络中所有计算机节点是以竞争的方式访问同一个共享介质，任何两台计算机同时发送数据都会产生冲突，这样的局域网其实是一个完整的冲突域。同时由于任何的计算机节点发送了广播报文，网络中所有的计算机都能够收到，因此网络同时也是一个广播域。现在仍较为常见的冲突域多是基于集线器构成的小型网络，如图 2-26 所示。

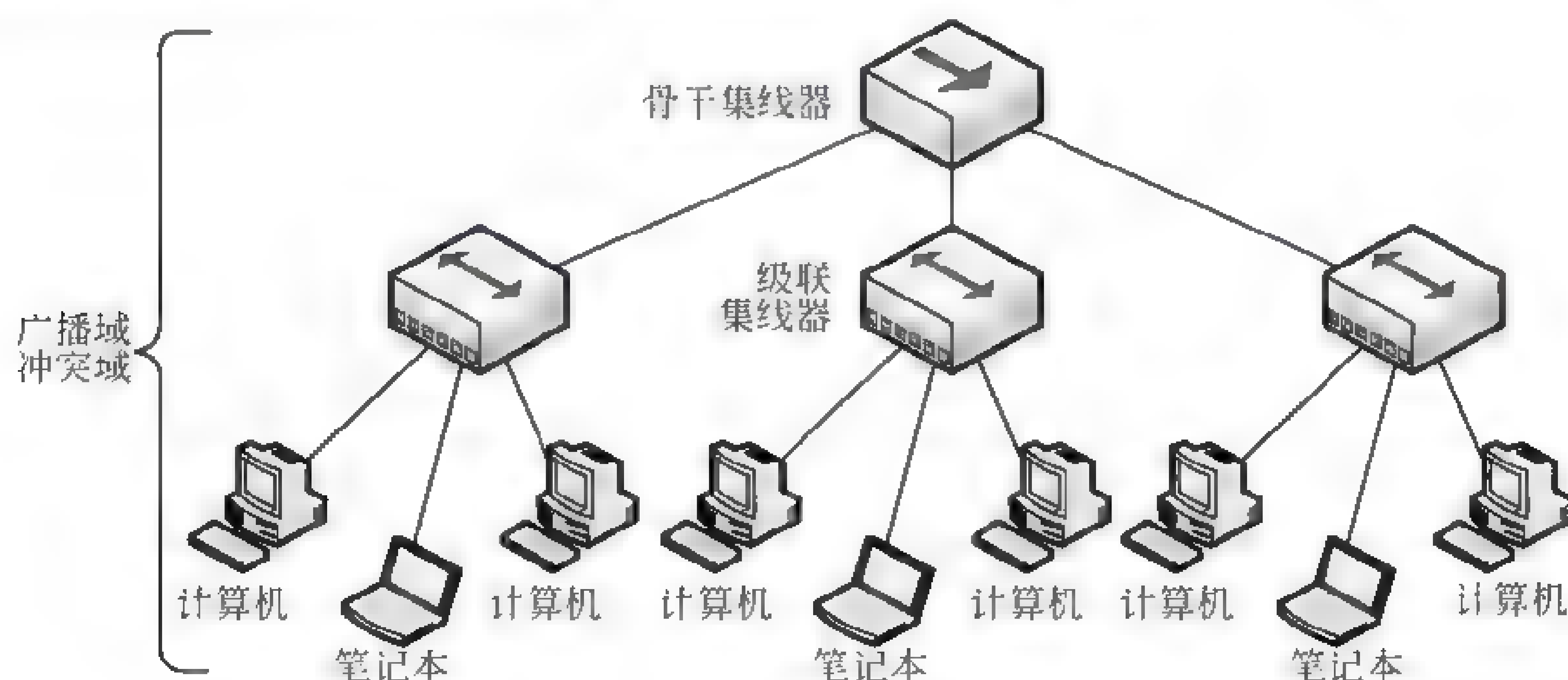


图 2-26　由集线器连接构成的冲突域

随着传统局域网络中计算机设备越来越多，网络中产生冲突的可能性也越来越大，当网络中计算机数量超过一定数量后，冲突就会导致整个网络通信处于瘫痪状态。为了避免这种情况，可以借助于特定的网络设备，把网络划分为多个冲突域，将冲突的范围

限制在多个冲突域内，这样只有在冲突域内的两台计算机同时发送数据才会产生冲突；同时，网络中任何的节点发送广播报文，网络中的其他计算机都可以接收到，所以这个网络仍然是一个广播域。将一个广播域划分为多个冲突域的网络设备是网桥或者交换机，目前较为常见的是利用交换机连接多个冲突域，如图 2-27 所示。

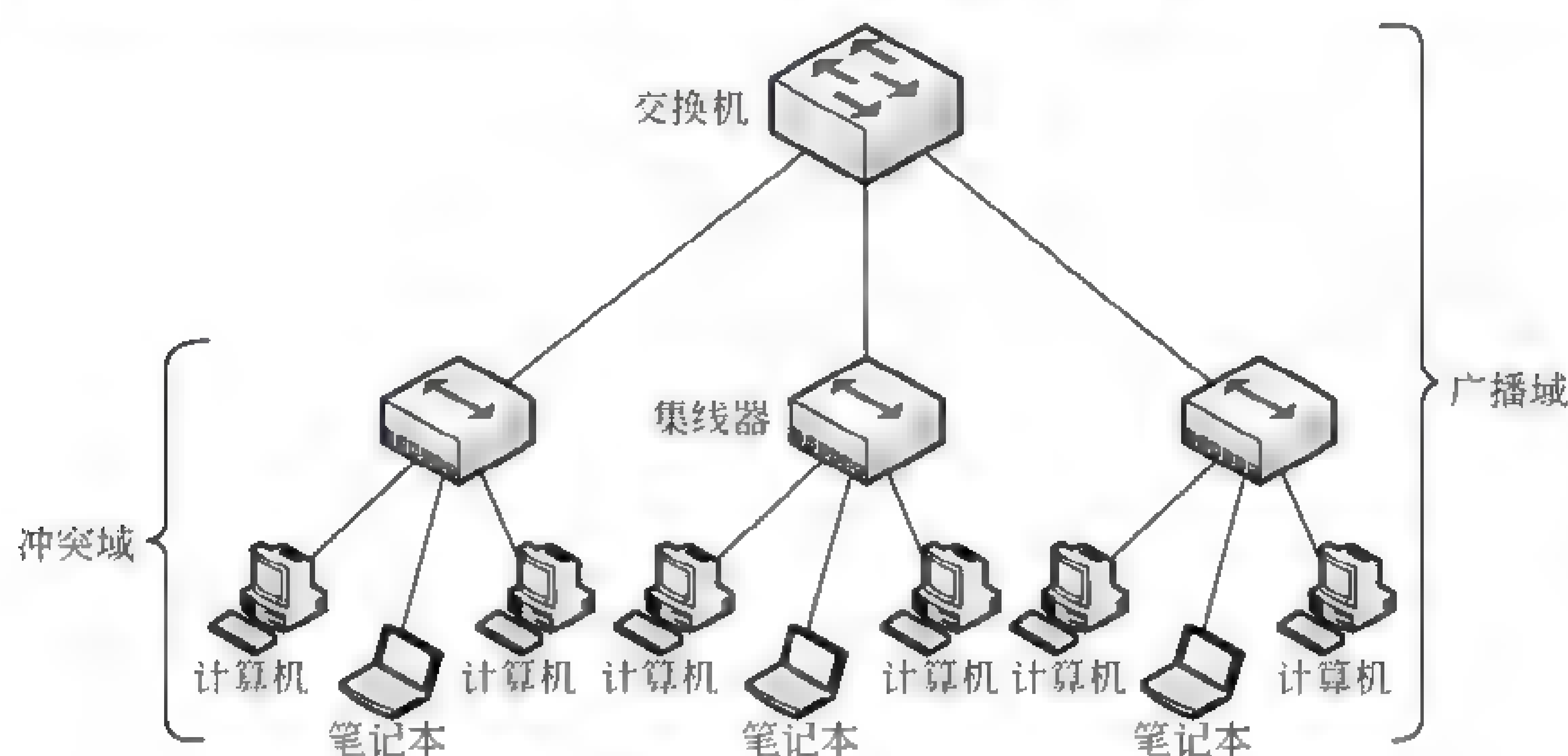


图 2-27　通过交换机划分的多个冲突域

在图 2-26 中，整个网络所有计算机设备共享 10M 带宽，而在图 2-27 中，每个集线器形成的冲突域共享 10M 带宽，而交换机实现了多个冲突域之间独占 10M 带宽，从而大大提高了网络的有效带宽。

随着交换技术的发展，网络中的共享设备逐步退出应用，随着“交换到桌面”的实现，冲突域逐步缩减为交换机的一个端口；但整个网络仍然是一个广播域，由于广播域内计算机数量增加，网络中产生的广播报文会越来越多，会形成广播风暴并消耗大量的网络交换容量；为避免这种情况的发生，可以将网络划分为多个广播域，限制广播风暴的影响范围。在网络中划分广播域可以采用两种方法，一种方法是采用交换机上提供的虚拟局域网（VLAN）技术，另外一种方法是采用路由器连接多个交换机形成的广播域。

VLAN 技术结合三层交换技术是当前建设园区网络的主流方式，局域网内部的多台交换设备划分为多个 VLAN，多个 VLAN 之间通过带有路由功能的三层交换设备互连，如图 2-28 所示。

为了建立隔离的广播域，必须在第三层对网络进行网段划分，三层交换设备或路由器有效地将常规网络通信和广播式网络通信限制在每个网段内，只引导网段间的通信，从而提高了整个网络的有效吞吐能力。

2）局域网通信流量边界

冲突域和广播域由不同的局域网络设备创建。冲突域的创建主要由传统的共享性设

备和共享性介质完成，而广播域创建除冲突域设备之外还可以借助于交换式设备完成。由于冲突域的特殊性，不可能出现一套共享物理设备中存在两个以上的冲突域的情况；因此冲突域的边界不能由共享性设备完成，主要是由路由或交换性设备构建，所以冲突域边界只能采用物理边界方式。而广播域建设中，由于 VLAN 技术的应用，在一套物理的交换设备中，可以同时存在多个相互之间隔离的逻辑广播域， 所以广播域边界可以采用物理边界和逻辑边界两种方式。

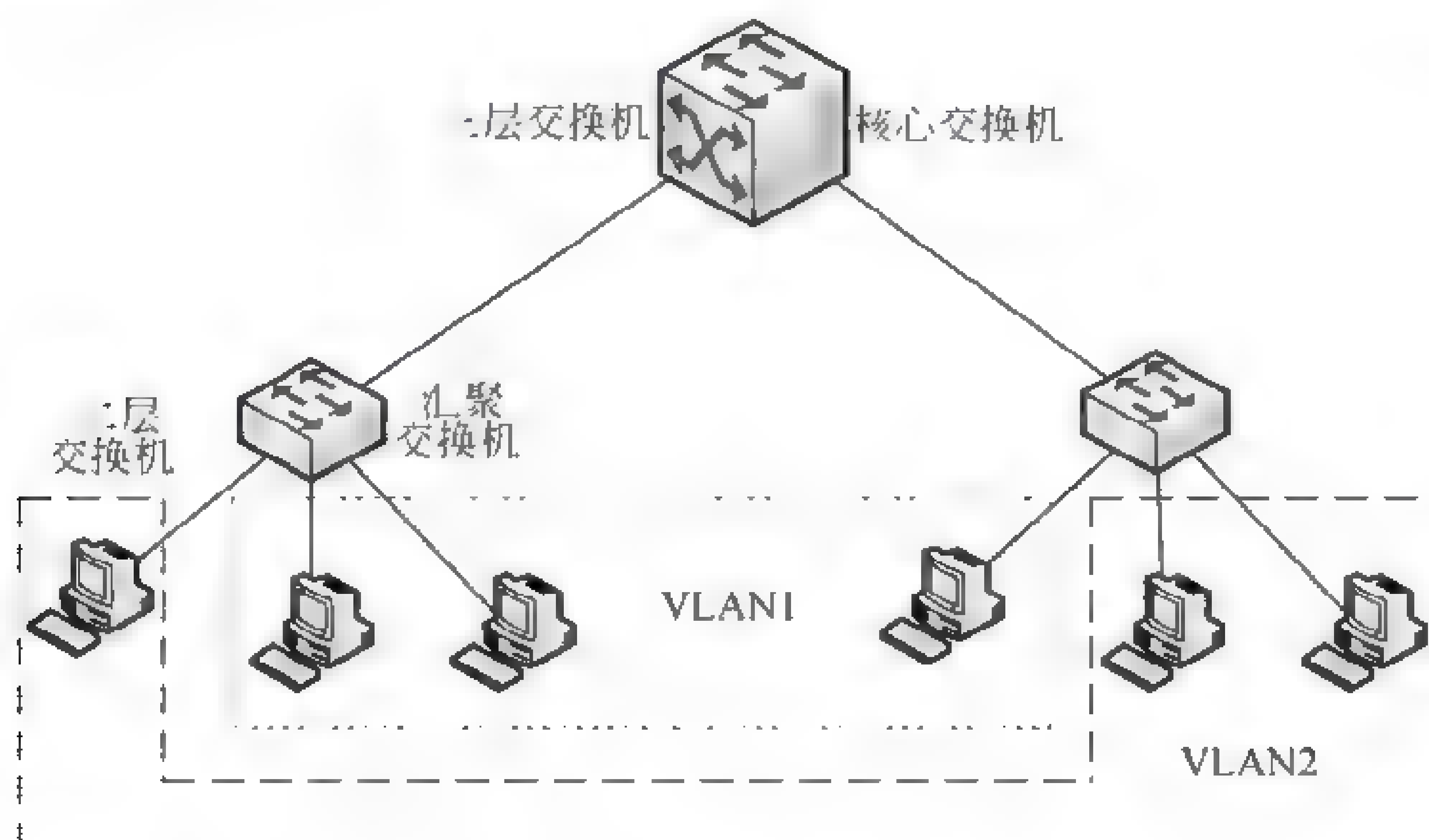


图 2-28　多个广播域划分

随着交换技术在局域网络中的应用，冲突域逐渐退出应用领域并缩减为交换机上的一个端口，在当今的局域网络中，除了较为特殊或者陈旧的网络工程，基本上都是以广播域建设为主的。

3）广播域物理边界

广播域的边界是局域网广播报文可以传递到的边界，通常情况下是网络设备的端口或者网卡。 在传统局域网中，划分广播域边界的设备是路由器，一般情况下路由器的一个端口就是一个独立的物理广播域。通过路由器，可以较为清晰地完成广播域的物理边界划分，并且可以真正隔离网络广播风暴产生的网络拥塞，如图 2-29 所示。

在进行通信规范分析时，如采用物理边界，则各广播域的负载是独立的，不会产生叠加效应，广播风暴效应也不会相互影响，但是网络管理工作量较大。

4）逻辑边界

在现代交换式局域网中，VLAN 技术对来自于不同广播域的数据帧进行数据封装，在一套交换设备中进行存储转发时，相互之间不会产生影响，因此可以实现多个虚拟广播域在一套物理交换设备中的共存。VLAN 的划分方式存在基于设备端口、物理地址、网络地址、策略等多种方式，所以广播域的划分不再是静态的，而是动态变化的；另外

由于多个 VLAN 是共存关系，一个 VLAN 的广播帧虽然不会传播至其他 VLAN，但由于共用交换设备，所有 VLAN 需要共享交换设备的交换容量，所以当一个 VLAN 产生广播风暴导致交换设备阻塞时，也会对其他 VLAN 产生间接影响。

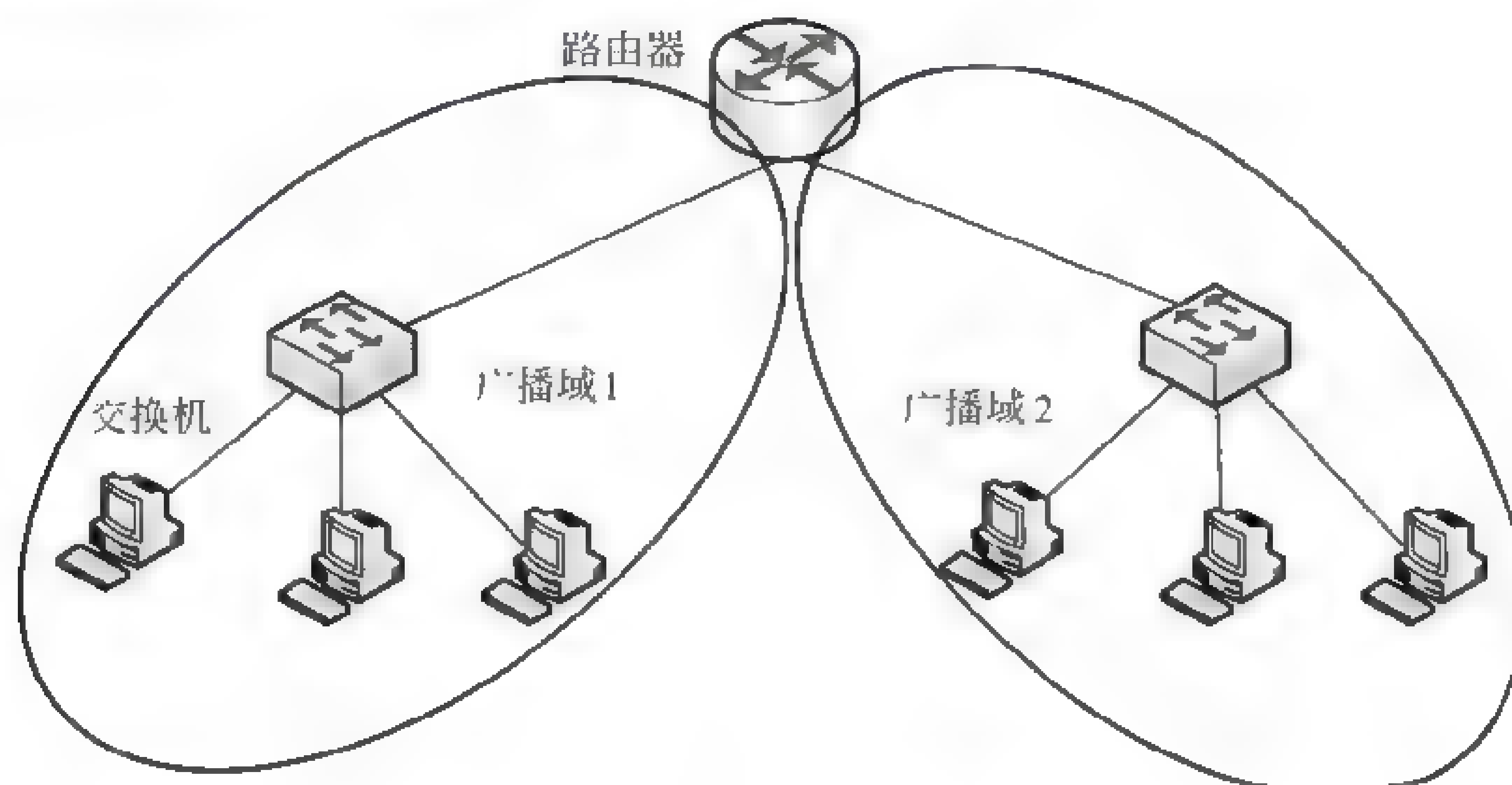


图 2-29 广播域物理边界

基于网络设备端口的 VLAN 划分方式是应用最广、最易于管理的方式，这种方式划分的广播域是静态的，因此在网络设计中，除非特殊的用户需求，都采用这种方式划分广播域。在进行通信规范分析时，应以基于端口的划分方式为分析依据，分析广播域的负载是如何叠加至网络设备的。

图 2-30 就是一个典型的广播域逻辑边界划分，采用基于端口的划分方式，广播域的边界是交换机上划归 VLAN 的端口；局域网中的核心交换机承载着多个 VLAN 的通信负载，是所有 VLAN 通信流量的总和，而会聚交换机则根据承载的广播域内节点数量不同而不同。

通过两种通信边界的分析，可以看出它们对通信规范分析工作的影响是不一样的。

2．广域网通信边界

传统的广域网是由通信线路所形成的点对点网络，在这些单纯的点对点网络中，由于点对点线路的通信都是独立并且有通信服务质量保障，所以并不存在通信边界问题。但是随着网络规模的不断发展，广域网络的情况越来越复杂，路由规划则成为广域网流量负载分布的关键。广域网的通信边界，主要由路由的自治系统、路由协议中的域和各局域网构成。

1）自治系统

路由的自治系统（Autonomous System，AS）是一个或多个互联的网络，其最重要的特点就是自治系统有权自主地决定在本系统内应采用何种内部路由协议，一个自治系统内的所有网络一般都属于一个行政单位（例如，一个公司，一所大学，政府的一个部

门，等等）来管辖。

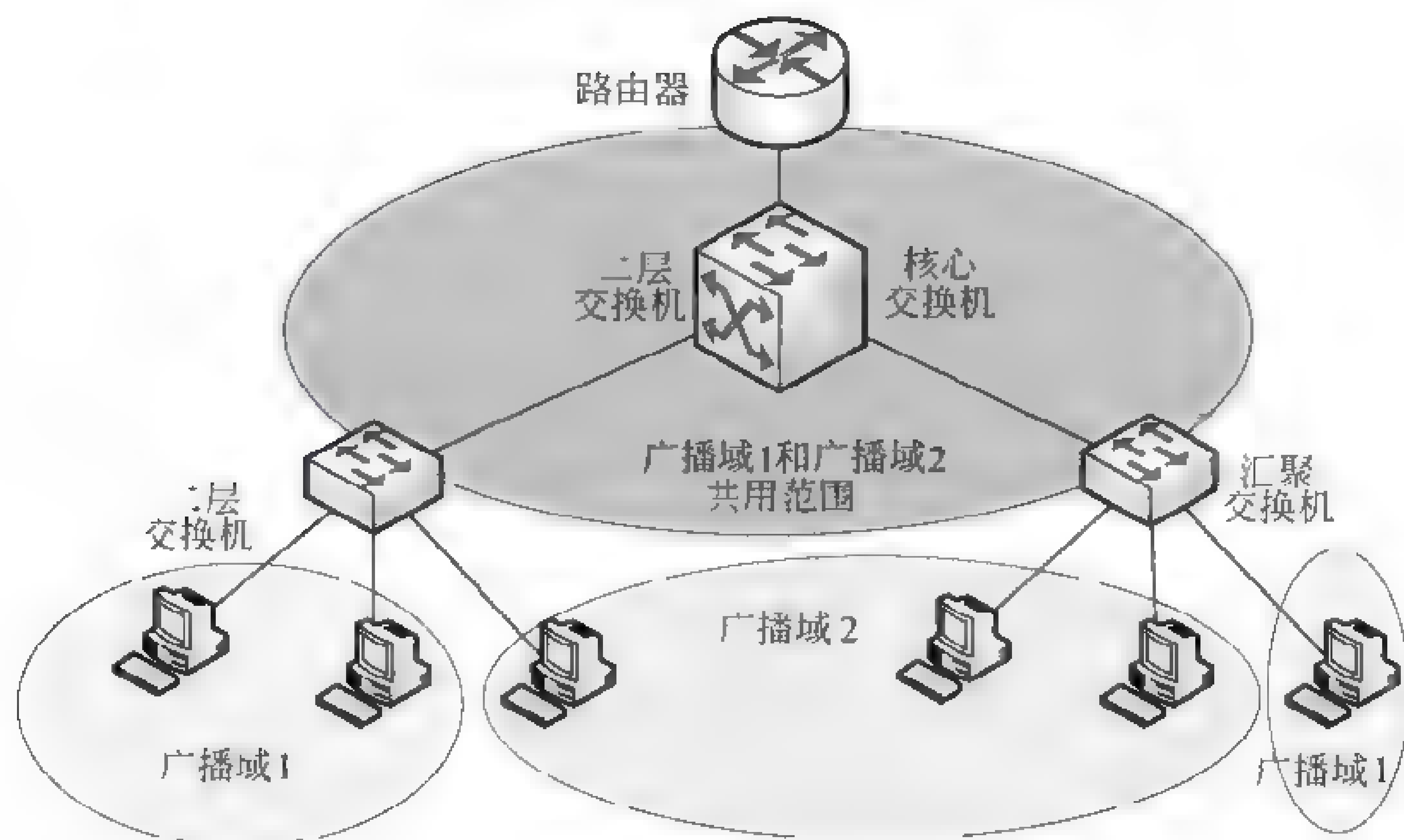


图 2-30　广播域逻辑边界

路由自治系统是天然的广域网通信边界，每个路由自治系统都拥有自己的自治系统号码，而系统的边界设备主要是高端路由设备。在这些自治系统边界路由器间运行的路由协议被称为外部网关协议（External Gateway Protocol，EGP）；而在自治系统内部运行的路由协议被称为内部网关协议（Interior Gateway Protocol，IGP）。一旦确定路由自治系统的边界，在进行路由自治系统的通信规范分析时，主要是分析从自治系统内部发往其他自治系统的流量，以及从其他自治系统流向本自治系统的流量。

2）路由算法区域

内部网关协议中应用较广的路由协议是开发最短路径优先协议（Open Shortest Path First，OSPF），该协议适用于网络规模较大的路由自治系统，需要将自治系统内的网络划分为多个域；域的划分方式是将所有运行 OSPF 的路由器人为地分成不同的组，以区域 id 来标示；在 OSPF 中，路由域存在骨干域（即 0 号域）和非骨干域，其中连接不同域的路由器即路由域的边界，被称为区域边界路由器（Area Border Router，ABR）。

3）局域网

自治系统内部的粒度最小的系统就是一个局域网络；在现代网络中，这种局域网络不会是一个广播域，而是一个通过内部路由设备互连起来的多个广播域；这种网络属于自治系统，但是与其他局域网络存在明显的边界路由器，该局域网的网络地址，在经过边界路由器对外时，会宣布为一个网段，而在内部则由内部设备宣布为多个子网段；因此，局域网络的边界路由器在不由路由协议划分区域的情况下，就是局域网的通信边界。

通过以上的分析，可以看出广域网络中的各种通信边界全部是由各种路由器来实现的，图 2-31 是一个各种路由器承担通信边界的示意图，而图中的自治系统边界路由器、

区域边界路由器、局域网路由器都是广域网的通信边界，在进行通信规范分析时，应针对这些边界设备进行仔细的流量分析。

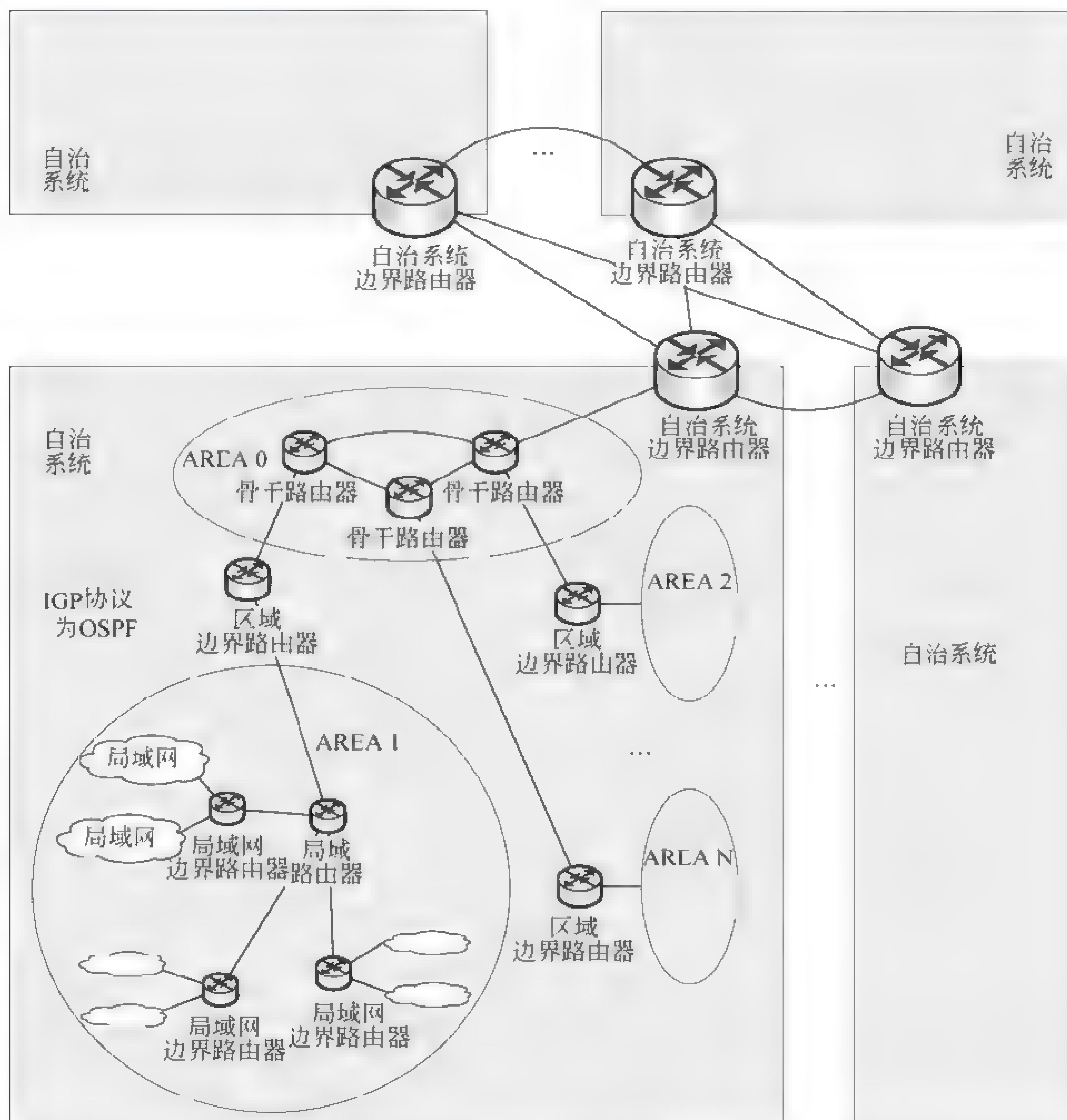


图 2-31 广域网中的各种边界路由器

3．虚拟专用网络通信边界

VPN（Virtual Private Network，虚拟专用网）的含义有两个，一是 VPN 是建立在现有物理网络之上，与物理网络具体的网络结构无关，用户一般无须关心物理网络和设备；二是 VPN 用户使用 VPN 时看到的是一个可预先设定的动态的网络。Private Network 的含义也有两个，一是表明 VPN 建立在所有用户能到达的公共网络上，特别是 Internet，也包括 PSTN、帧中继、ATM 等，当在一个由专线组成的专网内构建 VPN 时，相对 VPN

这也是一个“公网”；二是 VPN 将建立专用网络或者称为私有网络，确保提供安全的网络连接，它必须具备几个关键功能：认证、访问控制、加密和数据完整。

实现 VPN 的协议分为三种，第一种是工作于第二层数据链路层的 L2TP 等隧道协议，第二种是工作于第三层网络层的 IPSec、GRE 等隧道协议，第三种是依据标签封装机制而形成的 MPLS VPN 技术。无论是哪种技术，都必须采用图 2-32 的网络架构。

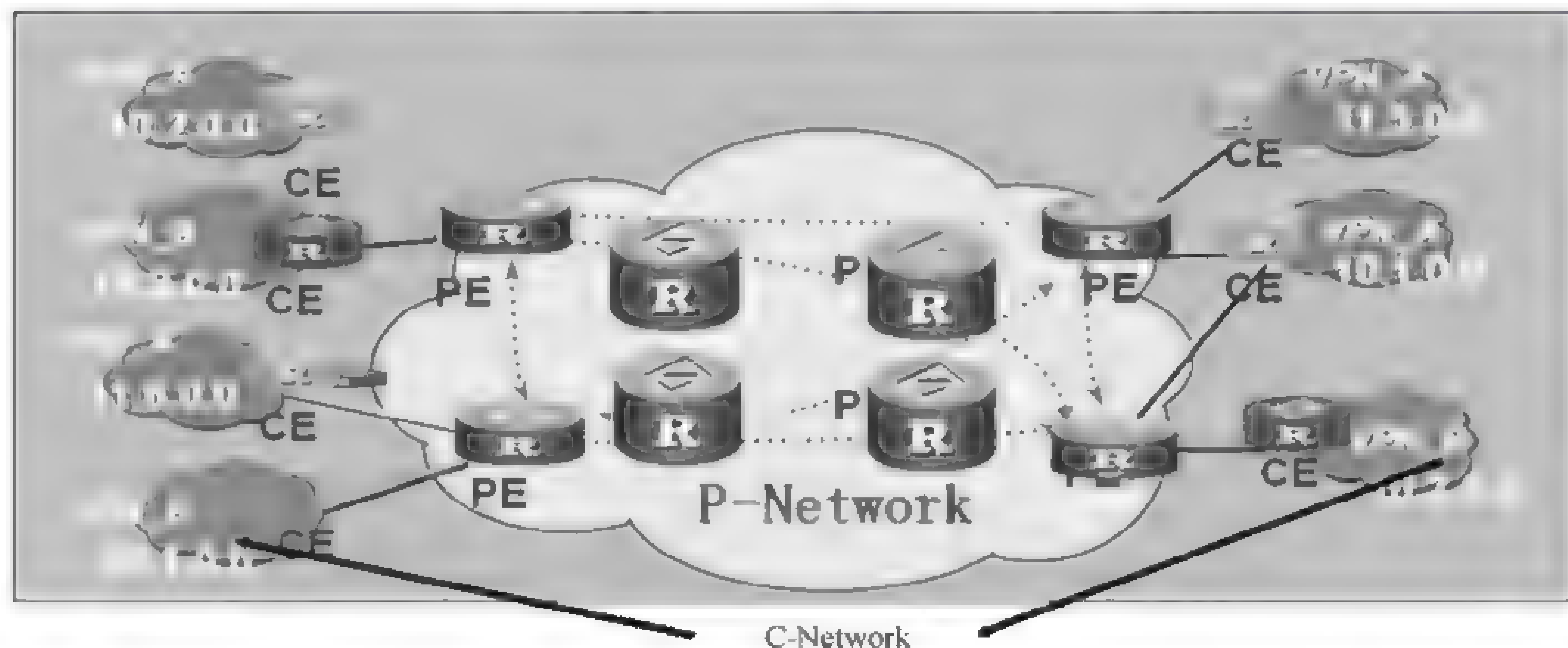


图 2-32　VPN 网络结构

在图 2-32 所示的各种路由器中，CE（Custom Edge）是直接与服务提供商相连的用户设备，PE（Provider Edge Router）指骨干网上的边缘路由器，与 CE 相连，主要负责 VPN 业务的接入，P （Provider Router）指骨干网上的核心路由器，主要完成路由和快速转发功能，由于网络规模不同，网络中可能不存在 P 路由器，PE 路由器也可能同时是 P 路由器。

无论在设计广域网络的 VPN 时采用哪种技术，无论形成 VPN 的结构是点对点（point-to-point）还是中心辐射状（hub-spoke），都会存在 CE 和 PE 路由器，而 PE 路由器就是 VPN 的通信边界，在进行 VPN 通信规范分析时，主要是统计各 CE 之间的流量形成对 PE 设备的传输容量要求。需要注意的是，这些通信流量在计算时需要考虑到加密算法、标签封装所产生的额外传输容量要求。

2.4.4　通信流量分布的简单规则

在通信规范分析中，最终的目标是产生通信量，其中必要的工作是分析网络中信息流量的分布问题。在整个过程中，需要依据需求分析的结果来产生单个信息流量的大小，依据通信模式、通信边界的分析，明确不同信息流在网络不同区域、边界的分布，从而获得区域、边界上的总信息流量。

对于部分较为简单的网络，可以不需要进行复杂的通信流量分布分析，仅采用一些

简单的方法，例如 80/20 规则、20/80 规则等；但是对于复杂的网络，仍必须进行复杂的通信流量分布分析，见第 2.4.5 节通信量分析的步骤。

1．80/20 规则

80/20 规则是传统网络中广泛应用的一般规则。80/20 规则是基于这样的可能性：在一个网段中，通信流量的 80%是在该网段中流动，只有 20%的通信流量是访问其他网段，如图 2-33 所示。

利用 80/20 规则进行通信流量分布的思路：对一个网段内部的通信流量，不进行严格的分布分析，仅仅是根据对用户和应用需求的统计，产生网段内的通信总量大小，认为总量的 80%是在网段内部的流量，而 20%是对网段外部的流量。

80/20 规则不仅仅是一种设计思路，也是一种特殊的优化方法，通过这种方式可以限制用户的不合理需求，是最优化地使用网络骨干和使用昂贵的广域网链路的一种行之有效的方法。例如，对于核心交换机容量为 100Mbps 的局域网络来说，其局域网至外部网络的带宽应限制在 20Mbps 以内。

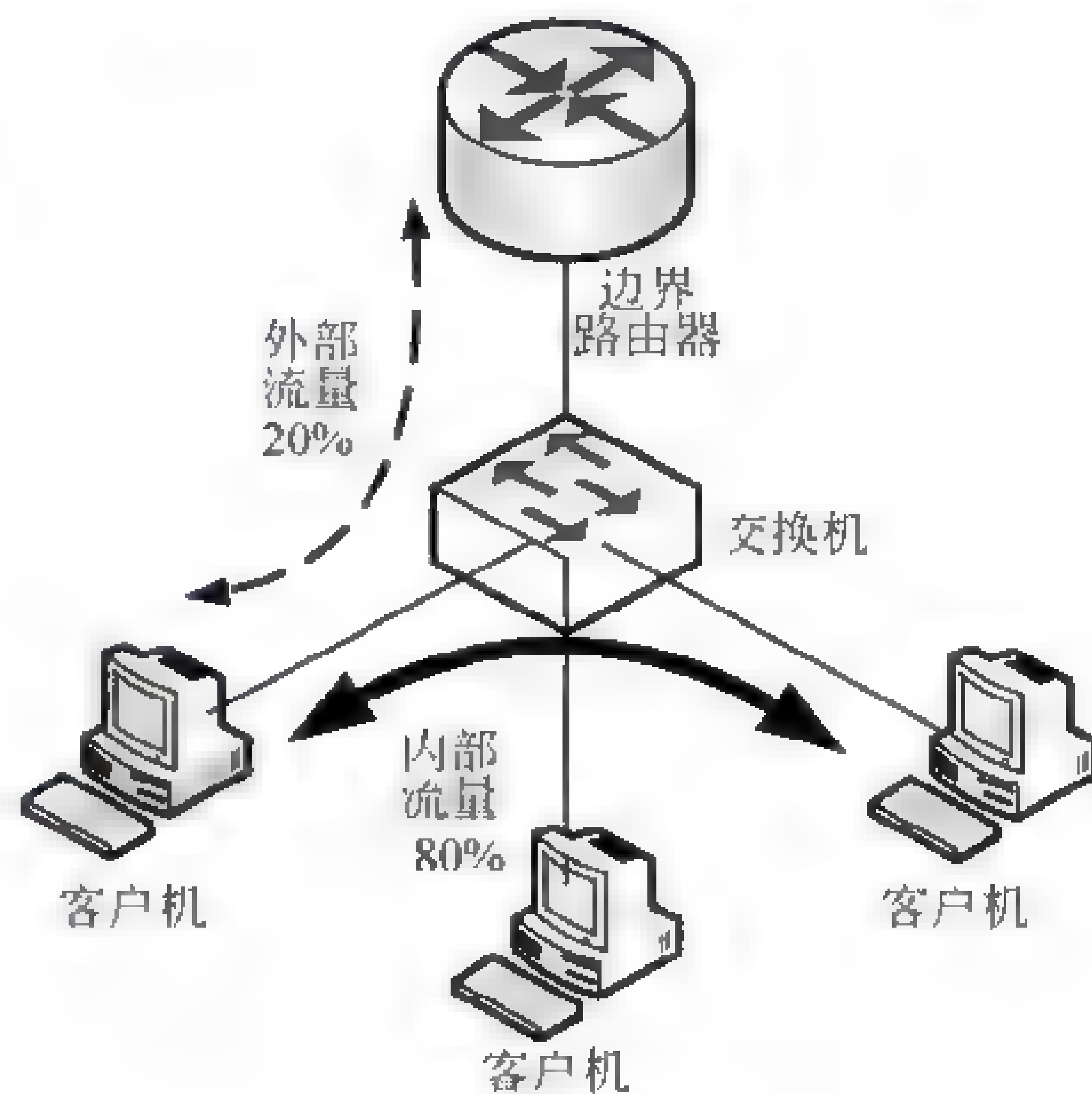


图 2-33　80/20 规则

80/20 规则适用于内部交流较多、外部访问相对较少、网络较为简单、不存在特殊应用的网络或网段。

2．20/80 规则

随着互联网络的发展，一些特殊的网络不断产生，例如小区内计算机用户形成的局域网络、大型公司用于实现远程协同工作的工作组网络等；这些网络的特征就是：网段的内部用户之间相互访问较少，大多数对网络的访问，都是对网段外的资源进行访问；对于这些流量分布恰好位于另一个极端的网络或网段，可以采用 20/80 规则。

利用 20/80 规则进行通信流量分布的思路是：根据对用户和应用需求的统计，产生网段内的通信总量大小，认为总量的 20%是在网段内部的流量，而 80%是对网段外部的流量。

需要注意的是，虽然 80/20 规则和 20/80 规则是一些简单的规则，但是这些规则是建立在大量的工程经验基础上的，另外通过这些规则的应用，可以很快完成一个复杂网络中大多数网段的通信流量分析工作，可以合理减少大型网络中的设计工作量。

2.4.5　通信流量分析的步骤

对于复杂的网络，需要进行复杂的通信流量分析，通信流量分析从对本地网段上和

通过网络骨干某个特定部分的通信流量进行估算开始，可采用如下步骤：

① 把网络分成易管理的网段。

② 确定个人用户和网段应用的通信流量。

③ 确定本地和远程网段上的通信流量。

④ 对每个网段重复步骤①～③。

⑤ 分析基于各网段信息的广域网和网络骨干的通信流量。

下面详细介绍各步骤的内容。

1．把网络分成易管理的网段

在通信流量分析的过程中，首要任务是依据需求阶段的网络需求、分段需求、工程经验将网络工程划分成若干个物理或者逻辑网段，并进行编号，同时选择适当的广域网拓扑结构，最终形成相应的各类网络边界；然后，从估算每个网段的通信模式、通信容量开始，分析在这些部分之间通信信息的流动方式；最后才产生通信流量。

网段划分需要根据用户的需求；对于升级的网络，可以对现有网段划分方式进行改进，形成新的划分方案；对于新建网络，则是和网络管理员一起商量网段划分方式；一般情况下，是按照工作组或部门来划分网段，因为相同工作组或部门中的人们通常使用相同的应用程序，并且具有相同的基本需求。

由于网段主要属于局域网络范畴，在进行分析工作前，需要确定网段的局域网通信边界；如果网段的通信边界是物理边界，则这个网段是需要独立进行分析的；而如果多个网段的通信边界是逻辑边界，则这些网段不需要独立进行分析，而作为一个整体网段来进行分析。

无论是物理网段分析，还是多个虚拟网段构成的整体网段分析，都可以采用局部分析法；局部分析法的实质在于只关注一个网段，并将该网段边界外的其他部分内容等同于一个外部网络来进行分析工作。

图 2-34 是一个较为复杂的网络，其中路由器 A 是一个局域网的物理边界；路由器 C 连接的局域网络较为复杂，存在着多个 VLAN，这些 VLAN 的通信边界是逻辑的，而路由器 C 则是这些 VLAN 和其他区域的共同物理边界。

在运用局部分析法时，需要对整个网络进行抽象化，形成图 2-35，其中左图和右图分别是路由器 A 所连接的物理网段和路由器 C 所连接的多个逻辑网段的局域分析法抽象图。

2．确定个人用户和网段应用的通信流量

在通信流量分析中，第二步是复查需求说明书中的业务需求、用户需求、应用需求、网络需求部分的内容，并根据通信流量的分析进行再次确定。在需求收集阶段，已经通过了用户对各种应用程序的估算使用量，其中反映流量的主要是应用需求和网络需求；但是这些估算使用量不仅仅包含网络流量，另外也没有根据通信模式进行流量分布分析；本步骤的工作在于将需求分析中不同格式的统计表格，再次确认后，根据通信模式，转化为统一的流量表格，以便于开始后续的分析工作。

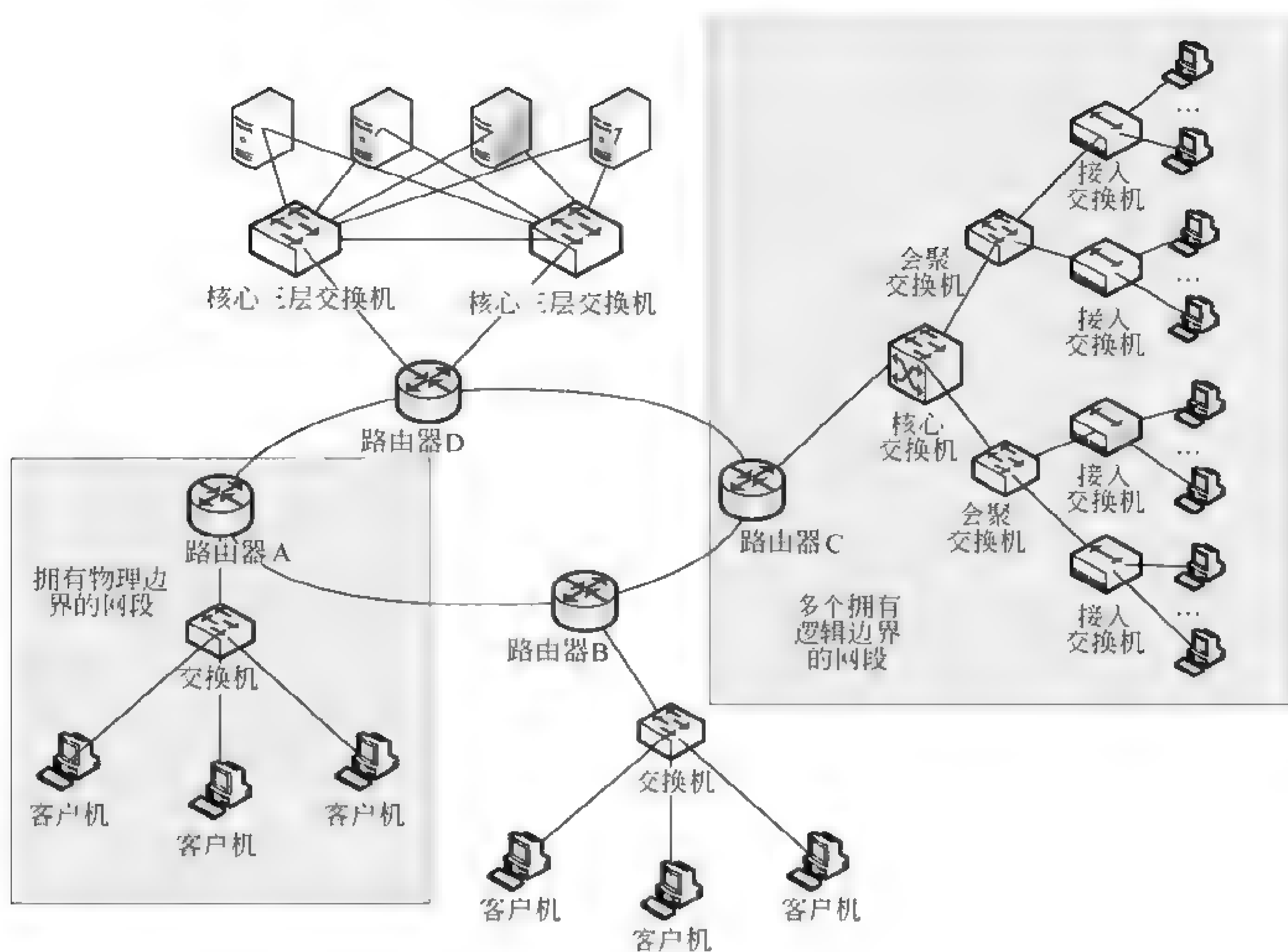


图 2-34　一个复杂网络示意图

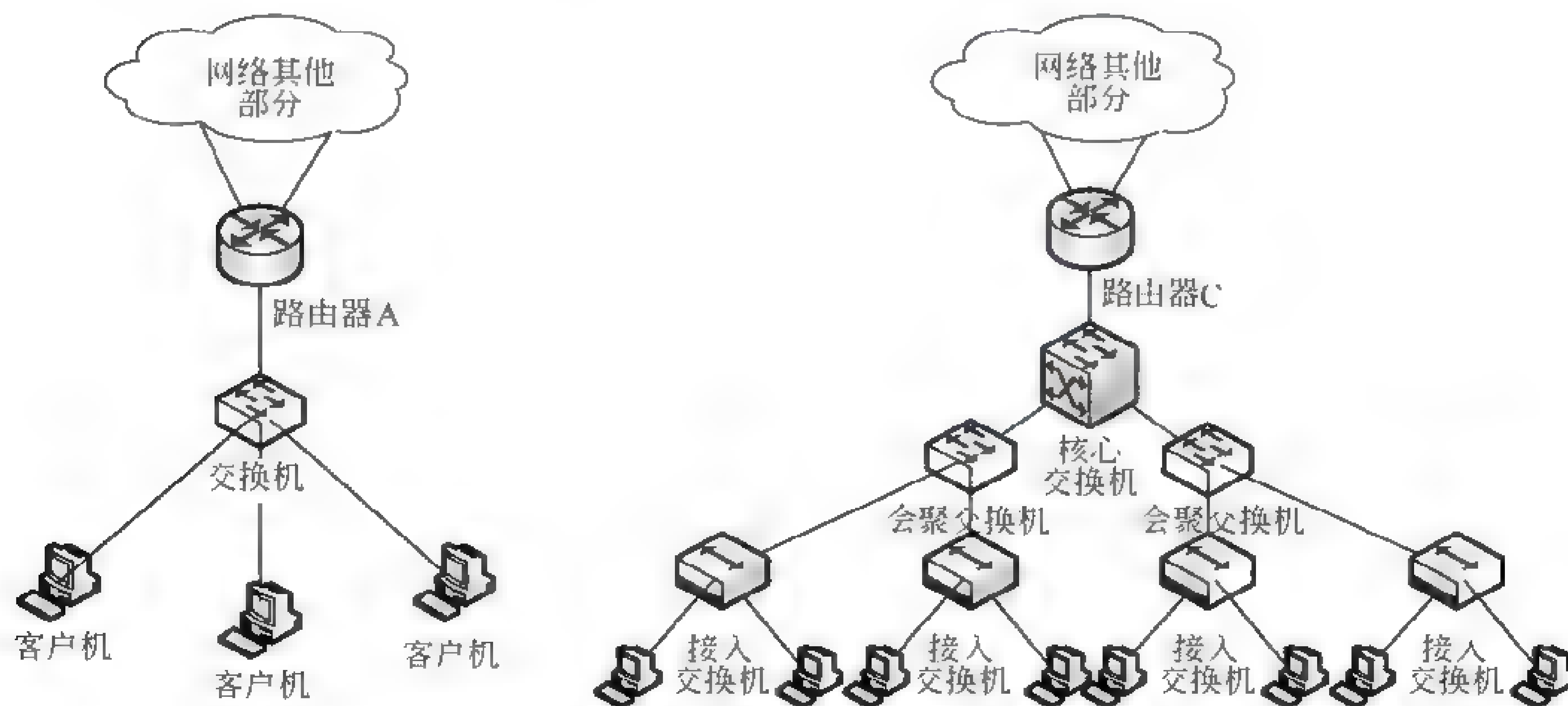


图 2-35　局部分析法所形成的抽象图

3．确定本地和远程网段上的通信流量分布

在第一步确定网段、第二步确定单个应用的模式流量后，确定本地和远程网段上的通信流量分布是分析工作的第三步。该步骤的重要任务是明确多少通信流量存在于网络内部，而多少通信流量是访问其他网段。下文以一个拥有物理边界的网段为例，借助于前两步的分析结果，进行通信流量分布分析。

假设一个专用网络中拥有 4 个物理网段，编号为 1～4 号，这 4 个网段直接通过路由器进行连接，如图 2-36 所示。其中，网段 1 为整个网络的核心网段，所有的服务器都托管在网段 1，而网段 2～网段 4 为普通的工作网段。

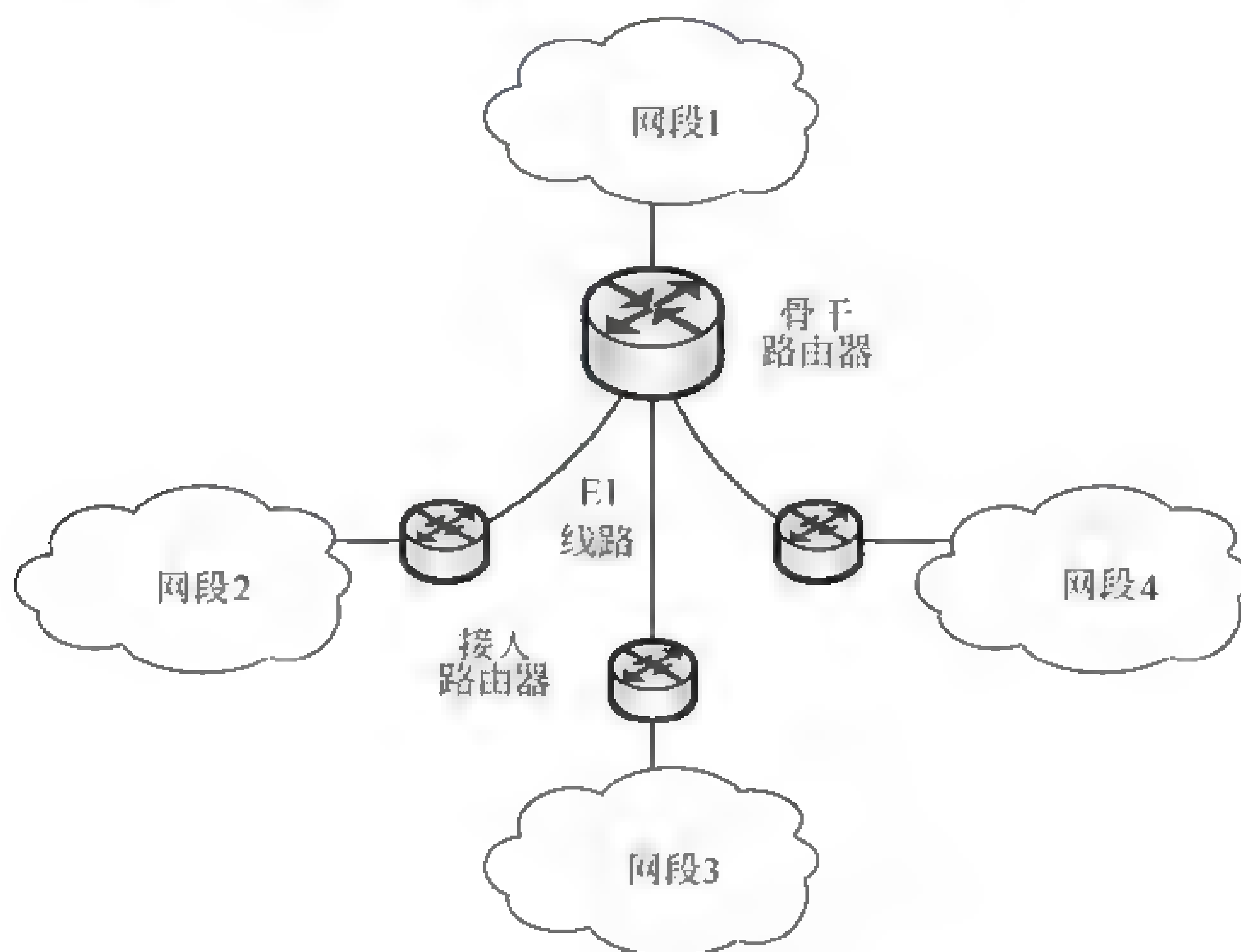


图 2-36　网络示意图

对网段 2 进行分析，网段 2 中的用户主要是使用以下几种应用。

- 工作邮件：用户需要通过邮件客户端访问置于网段 1 的邮件服务器。
- 办公自动化系统：办公系统应用服务器位于网段 1，BPS 模式提供服务。
- 生产管理系统：服务器位于网段 1，BPS 模式提供服务，主要用于满足生产工作管理需要。
- 文件共享服务：服务器位于网段 1，主要采用 Windows 网络文件系统提供 C/S 服务。
- 视频监控：用户可以互相调阅不同网段的视频监控流，不需要经过流媒体服务器的管理，属于典型的 P2P 应用。
- 内部交流：指用户借助于部分局域网通信软件，进行内部交流。

在需求分析中，可以形成表 2-11 所示的表格。

表 2-11 应用需求分析表

应 用 名 称	平均事务量大小	平均用户数	平均会话长度	每个会话发生的事务数量	网络模型
工作邮件	1MB	200	1 分钟	2	C/S
办公自动化系统	0.02MB	400	1 分钟	4	BPS
生产管理系统	0.05MB	200	1 分钟	8	BPS
文件共享服务	100MB	100	10 分钟	1	C/S
视频监控	400MB	20	1 小时	1	P2P
内部交流	0.01MB	800	1 分钟	4	P2P

计算出应用需要传递信息的速率，可以根据公式：应用总信息传输速率＝平均事务量大小×每字节位数×每个会话事务数×平均用户数/平均会话长度。

根据该公式，计算出结果如下。

工作邮件：1×8×2×200/60＝53Mbps

办公自动化系统：0.02×8×4×400/60≈4.3Mbps

生产管理系统：0.05×8×8×200/60≈10.7Mbps

文件共享服务：100×8×1×100/600≈133.3Mbps

视频监控：400×8×1×20/3600≈17.8Mbps

内部交流：0.01×8×4×800/60≈4.3Mbps

（注：不同的计算方法，需要调查和测试的网络指标不同，本文中仅为一个简单示例。）

同时，由于三个工作网段基本上是类似网段，用户在三个网段的分布基本一致，所以网段 2 所承担的各应用的比例都是 1/3，各应用的信息传递速率是总速率的 1/3。

由于各应用的通信模式不同，各应用在网段 2 中的通信流量分布也不同，分析通信模式后形成表 2-12 所示的表格。

表 2-12 应用流量分布表

应 用	通 信 模 式	通 信 流	网段分布	源网段	目的网段	估 算 流 量
工作邮件	客户机-服务器	①客户机至服务器	发出网段	2	1	53×50%＝26.5
		②服务器至客户机	进入网段	1	2	53×50%＝26.5
办公自动化系统	浏览器-服务器	①客户机至服务器	发出网段	2	1	4.3×20%＝0.86
		④服务器至客户机	进入网段	1	2	4.3×80%＝3.44

续表

应　　用	通信模式	通　信　流	网段分布	源网段	目的网段	估算流量
生产管理系统	浏览器-服务器	①客户机至服务器	发出网段	2	1	10.7×20%=2.14
		④服务器至客户机	进入网段	1	2	10.7×80%=8.56
文件共享服务	客户机-服务器	①客户机至服务器	发出网段	2	1	133.4×50%=66.7
		②服务器至客户机	进入网段	1	2	133.4×50%=66.7
视频监控	对等通信	①P2P 流	进出网段			17.8×66%=11.8
		①P2P 流	网段内部			17.8×33%=5.9
内部交流	对等通信	①P2P 流	网段内部	2	2	4.3×100%=4.3

注：由于工作邮件、文件共享服务的网络通信模式为客户机-服务器模式，属于双向流量大，因此在网段流量分布上应用的总流量在两个方向上各占 50%；办公自动化系统、生产管理系统属于浏览器-服务器模式，在估算时客户机至服务器按 20%进行估算，反向按 80%进行估算，在实际项目中可根据测试情况进行调整；内部交流主要在网段内部，不产生外部流量；视频监控主要是根据用户在网段比例，网段内部用户数量为总用户的 1/3，而其他网段则占 2/3。在本示例中没有考虑 TCP 协议、IP 协议封装所引起的流量，如需要考虑这些协议封装而增加的流量，则需要统计各应用的平均协议包长度，并根据协议包头长度和有效负载长度算出实际的网络层流量；例如假设经过统计或者经验，工作邮件的平均 IP 包长度为 1200B，则 IP 包头为 20B、TCP 包头为 20B，其余的为有效负载部分，则工作邮件客户端至服务器端应用流量实际产生的网络层流量为 26.5×1200/1160≈27.4Mbps。

基于以上分析，可以形成表 2-13 的总流量分布。

表 2-13　网段 2 总流量分布表

流量分布	源网段	目标网段	应用总流量	网络总流量
网段内部	2	2	5.9+4.3=10.2	10.2×64/56≈11.7
访问服务器	2	1	26.5+0.86+2.14+66.7=96.2	96.2×64/56≈110
服务器反馈	1	2	26.5+3.44+8.56+66.7=105.2	105.2×64/56≈120
外部 P2P	2	其他	11.8	11.8×64/56≈13.5

注：由于以太网的最小帧长为 64B，其中有效负载为 56B，因此可以根据这种极端情况计算出所需要的最大网络流量。

由表 2-13 可知，网段 2 内部的网络设备必须提供 13.5Mbps 的网络吞吐率，而网段 2 和网段 1 之间的往来流量分别为 110Mbps 和 120Mbps，由网段 2 访问其他网段的双向

流量为 13.5Mbps；则内部交换机的吞吐率必须大于 13.5Mbps，网段 2 的边界路由器必须提供大于 110+120+13.5＝243.5Mbps；而对于网段 2 的边界路由器，该路由器至内部交换设备的连接应提供正向 110+13.5/2＝116.75Mbps，方向 120+13.5/2＝126.75Mbps 的传输速率，则在设计时可以采用千兆以太线路并将线路的双向传输速率都限制在 200Mbps 以内。同时，表 2-13 可以作为广域网和网络骨干的计算依据。

需要注意的是，以上仅仅是根据用户需求、应用需求计算网络流量的一种示例，不同的设计人员采用的需求分析方式和表格不同，其计算的方法也不同，但是都可以获取网络层流量。例如有些设计人员喜欢用在线用户数量、每个在线用户的平均流量来进行计算；有些设计人员喜欢用应用的用户每秒事务量和事务量大小来计算流量；还有些设计人员会考虑峰值情况，并以峰值速率作为设计依据，以避免网络在峰值时段出现拥塞。

4．对每个网段重复上述步骤

对每个网段重复上述步骤，其中个人应用收集的信息是每一个应用和网段都要用到的；然后，确定每一个本地网段的通信量以及该网段对整个广域网和网络骨干的通信量。

5．分析基于各网段信息的广域网和网络骨干的通信流量

通过对每个网段的分析，除了形成各网段自身的通信要求外，还可以形成与本网段有关的广域网、骨干网的通信要求。不同网络工程中，用户对广域网拓扑结构的要求和建议不同，即使拓扑相同，信息的路由不同，对网络设备的要求也是不同的；因此对广域网和网络骨干的通信流量分析必须参考用户意见，并且应当做到灵活机动。

图 2-36 的网络较为简单，路由也不存在太多的灵活性，因此对广域网的分析也比较简单。由于网段 2～网段 4 的情况基本一致，用户数量也相同，所以网段 3 和网段 4 所产生的总流量分布也是一致的。对广域网的分析如下：

（1）骨干路由器至接入路由器连接的带宽要求为下行大于 126.75Mbps，上行大于 116.75Mbps。

（2）骨干路由器的吞吐量应大于三个接入路由器吞吐量的总和，也就是 243.5×3＝730.5Mbps。

（3）骨干路由器至网段 1 的连接主要承担各网段至网段 1 的流量，则该连接至网段 1 的带宽应大于 110×3＝330Mbps，反向的带宽应大于 120×3＝360Mbps，则该连接也必须采用千兆以太网线路，并可将线路的双向传输速率都限制在 400Mbps 以内。（注：外部 P2P 流量不需要经过该连接。）

在图 2-36 中，网络的骨干是由网段 1 构成，主要存放网络中的所有服务器，而所有的服务器都要满足应用的数据吞吐量需要，根据第二步中计算的各应用吞吐量需求，除了文件共享服务器为 133.4Mbps 之外，其他的都是 100Mbps 以内，因此普通的千兆交换机，可以满足应用的通信需求。

本示例中网络骨干的流量较为简单，服务器之间的交换流量较少，但对于较为复杂的骨干网络，需要进行仔细的流量分析。

6. 输出通信流量计算

通信流量计算完成后，要把它们整理总结成一份文件，该文件将成为最终的通信规范说明书中的一部分。同时，用这些新的信息来提高当前逻辑网络图的质量，标明广播域、冲突域和子网的边界。如果通过通信流量计算，表现出了定向通信模式，也应在图上标出。

2.4.6 网络基准

除了通过收集用户信息并计算通信流量的方法外，还存在更为精确的基于通信流量的计算法，即基准法。

基准法是通过测量一个网络的容量和效率来衡量网络性能要求的方法。通过网络的测试数据，可以发现网络中存在的问题，也可以把握网络发展趋势对网络性能带来的影响。对于升级的网络工程，基准法可替代通信流量计算法作为设计依据，也可以配合使用；对于新建网络工程，可以使用基准法中的仿真机制，作为设计工作的验证机制。

采用基准法测量需要专门的监视器设备和应用软件，但由于所需的硬件和软件较为昂贵，所以通常只依靠估算法来确定和记录网络的性能。但是，只要条件允许，最好能同时使用估算法和基准法。

1. 测试工具

传统的测试工具是局域网分析器。例如，网盟公司的探测器（Sniffer）、HP 公司的局域网顾问（LAN Advisor），另外互联网上存在大量的类似 Sniffer 软件，它们能够记录一个网段在给定时间内的通信信息。

另外还可以使用局域网仿真软件包，实现通过 PC 来监控网络的功能。软件包提供的工具如下：

- 网络镜像。
- 物理网络层管理。
- 网络设计。
- 网络规划和仿真。

1）设计与建模工具包

设计工具包的功能是模拟局域网在一定负载下的行为。只要提供用户数量、应用程序、通信链路等信息，工具包就能给出局域网性能的描述。一些工具包还可以评估特定应用程序产生通信量并绘制图表。同时，它们还包含各种网络设备（如网桥和路由器等）的信息库，设计人员可以在模型中直接插入设备，并对设备吞吐量和响应时间提供合理的估算。

2）仿真与测试工具包

局域网通信仿真包具有产生真实的局域网测试通信信息的功能。通过改变通信信息的大小和频率，就可以测出局域网的效率。仿真与测试工具包可以根据内置的客户机活

动函数，测试或评估局域网的性能。该工具包还可以用于监控各个局域网设备的行为，从而确定各个组成部分的延迟。

2．网络基准化

网络基准是对网络活动和行为的测试，通过对网络行为进行提前的预测，实现周期性测量，并形成一系列的参数指标。例如监测到高带宽应用时，应该在每个独立的网段、广域网链路以及网络骨干链路上运行独立的测试，获取基准测试指标值，这样就构成了整个网络的基准集。

按固定的时间间隔进行基准化可能产生相同的结果，因此应该随机进行网络基准化，以便获取全面情况，并及时发现问题。

Sniffer 是当前比较流行的网络分析工具，该类产品较多，产品的形式既可以是软件也可以是硬件，并且互联网上存在大量的开源自由软件，因此应用较广。

Sniffer 在局域网及广域网管理和基准化领域使用较多，下文将以 Network General Sniffer 为例介绍网络进行基准化的几个必要步骤，大多数 Sniffer 产品的功能都与其类似。

1）Sniffer 的功能

Network General Sniffer 是基准网络的一种常用的测量局域网活动的工具。它存在多种产品形式，可以是一个独立的硬件单元，也可以是纯软件。一台运行 Sniffer 软件设备的网卡必须与被分析的网络兼容。

（1）监视模式下的网络基准。

在一个网段上进行约 10 分钟的基准就能提供一次全面的安全检查，并且能提醒用户注意可能忽视的潜在问题，经常进行基准化能有效地防御问题的发生，并可在出现故障时及时协助修复。对于局域网络来说，基准能洞察到带宽的使用率、冲突率、循环冗余校对（CRC）错误的百分比、平均帧大小、协议分配、上层会话站点（和与之对话的站点）以及在一个网段之内的总站点数等情况。

（2）分析器模式下的故障诊断。

在出现故障时，Sniffer 是一个有效的分析工具，可以直接发现网络各层次上出现的异常，并直接提示用户，便于找到故障的根源。大多数 Sniffer 具有解释协议堆栈的能力，加上强大的过滤功能，使得它成了在网络基准化时的重要工具。

2）连接介质和基本操作

Sniffer 必须接入网络，并能够收集到网络中的数据才能完成基准化工作，因此必须和相关的网络子网实现物理连接，也就是 Sniffer 上必须安装与被基准化网络兼容的网卡。

网卡工作在正常状态下时，只接受三种类型的数据帧：第一种，目标地址和网卡地址相同；第二种目标地址为广播地址；第三种目标地址为组播地址。但是 Sniffer 为了能够收集网络中的所有数据帧，网卡必须能够接收到发送到网卡的所有数据帧，这种模式

被称为混杂模式。在共享网络中，网络上的数据帧所有网卡都可以接收到，因此将 Sniffer 的网卡设置为混杂模式，就可以完成网络中的数据帧收集工作。

在交换式局域网络中，交换机会根据数据帧的目标地址进行数据帧的存储转发，因此 Sniffer 设备的网卡即使工作在混杂模式，也只能接收到被转发到网卡的数据帧；为了让 Sniffer 设备可以在交换网络中完成基准化工作，交换机提供了通信流量镜像功能，可以将各端口流量复制到指定的端口，从而实现各种数据帧的收集工作。

在实施网络基准化工作时，必须完成 Sniffer 设备的网络接入和配置工作，在交换机上实现 Sniffer 设备接入时，必须选择合理的端口，至少要保证所有被监听数据端口的速率之和应小于 Sniffer 设备接入端口的速率。

3）监视器模式下的网络基准

网络基准是网络活动和性能的快照。基准提供了对网络性能的预测能力，也是对网络的监视，既可以周期性地进行，也可以在感兴趣的事件发生时进行。为了保证基准工作的效果，应该随机地对每个子网进行基准工作。

4）建立相关名称数据库

在现代网络中，网络中的节点都拥有自己网卡的 MAC 地址，在进行基准化工作时，会出现大量的网卡 MAC 地址。由于 48 位的网卡 MAC 地址难于记忆，因此可以对关键节点的 MAC 地址定制方便记忆的名字，而这些名字都存放在 Sniffer 的数据库中。

没必要给一个网络里所有的节点元素起名字，因为建立名称数据库只是为了识别那些最重要的组件或者节点，一旦建立了重要节点的名字，就可以方便地进行基准化工作，并快速确定存在问题的网络节点。

5）Sniffer 分析器

Sniffer 分析器能够监视或捕捉与之相连接的子网上的通信。分散的基准可在每一个独立的子网上运行，进而形成整个网络的一整套基准。

3．基准的解释

Sniffer 设备将根据收集到的数据帧，形成一系列记录网络行为的基准参数指标，这些参数指标构成了基准集合，常用的基准指标包括如下内容。

1）全局统计数据

全局统计数据将网络作为一个整体来描述所有来自被监控的站点的通信流，包括以下一些指标。

（1）站点数。

站点数是指在子网上能被 Sniffer 看到的子网上的站点总数，Sniffer 还可以列出每个站点的活动情况。

（2）平均利用率。

平均利用率描述某个站点已利用的带宽与可利用带宽的百分比。

（3）总帧数和总字节数。

从监控开始时刻，Sniffer 监控到的所有数据帧的总数和总字节数，并且可以根据特定的要求进行分类。

（4）物理层错误。

Sniffer 可以发现存在错误帧或 CRC 校验错误之类的物理层错误，用户可以根据错误信息发现问题的原因。

2）所有站点信息

Sniffer 可以记录每个站点的总帧数、错误数、字节数以及每个站点所占用的网络带宽百分比。

3）帧大小

帧大小是指帧的大小分布，大多数 Sniffer 都可以将所有监测到的帧按大小分类，这在识别协议和辨别网络有效性时很有用。

4）协议类型

Sniffer 可以分析接收到数据帧的协议类型，并根据协议的类型进行分类和统计工作，这些统计信息包括各种协议数据包占全部数据帧的百分比。

5）报警日志

报警与带宽利用率或错误有关。例如，它可以列出与带宽使用或误差相关的报警信息。

在许多情况下，列出报警信息表示已超出了一个事先规定的阈值，报警并不表示一定产生了错误，但是对网络问题的分析有一定的帮助。

6）全局历史记录

全局历史记录是每隔一定时间间隔进行规则采样的结果，它列出了日期/间、帧数、误码率、字节数和利用率，这是多次基准化所形成的累计值。

4．基准网络的操作

由于不同 Sniffer 产品的操作方式不同，本文对 Network General Sniffer 不进行详细的操作描述，用户可以按产品提供的用户手册进行操作。

5．测算共享资源的利用率

共享资源就是在网络中由多个用户共同分享的资源，如服务器和打印机等。了解设备的利用率对分析问题非常有效。在网络中的服务出现故障时，管理人员依据共享资源的利用率，就可以判断问题到底是来自于服务器，还是来自于网络，并给出正确的排错方案。

下列的各项都是可能会影响网络性能的原因，在测算共享资源利用率时，应关注这些内容。

- 发送端的应用程序。
- 发送端的 CPU 时钟速度。
- 发送端的输入输出（I/O）总线类型及数据速度。

- 发送端的操作系统（OS）类型。
- 发送端的任务数、执行数（CPU 利用率）。
- 发送端的存储器数。
- 发送端的网卡延迟。
- 局域网链路延迟。
- 广域网链路延迟。
- 协议堆栈。
- 网络互联设备的等待时间。
- 接收端的应用程序。
- 接收端的 CPU/时钟速度。
- 接收端的输入输出（I/O）总线类型及数据速度。
- 接收端的操作系统（OS）类型。
- 接收端的任务数、执行数（CPU 利用率）。
- 接收端的存储器数。
- 接收端的网卡延迟。
- SCSI 接口类型/速度。

6．测量工具

除了 Sniffer 这些专业测试工具之外，不同的操作系统也提供了不同的方法来测量共享资源的利用率。在 UNIX 操作系统上经常用命令行工具来测量 CPU 资源。在 Windows 平台上，存在着多个服务器资源监视工具，这些工具包括：

- 性能监视器。
- 任务管理器。
- 网络监视器。

1）性能监视器

性能监视器可以监控并分析 Windows 操作系统的运行情况。它除了记录服务行为的实时图外，还能将这些统计表记入日志并进行重播，且以报表的形式显示出来，或者在量度超出或落后于预先设置的阈值时产生提示信息，性能监视器窗口如图 2-37 所示。

2）任务管理器

任务管理器是一个综合性的工具，其功能是监视应用软件、任务和 Windows 系统的主要性能量度。任务管理器能提供在工作站上运行的每个应用软件和进程的详细信息以及内存和 CPU 的使用情况。对于终止不响应的程序和进程，任务管理器将其操作变得非常简单，同时提高了系统的可靠性，如图 2-38 所示。

3）网络监视器

分析和维持网络自身的完整性是管理网络的一个基本要素。网络监视器提供了识别网络通信模式、测试网络以及查明网络故障点的功能。

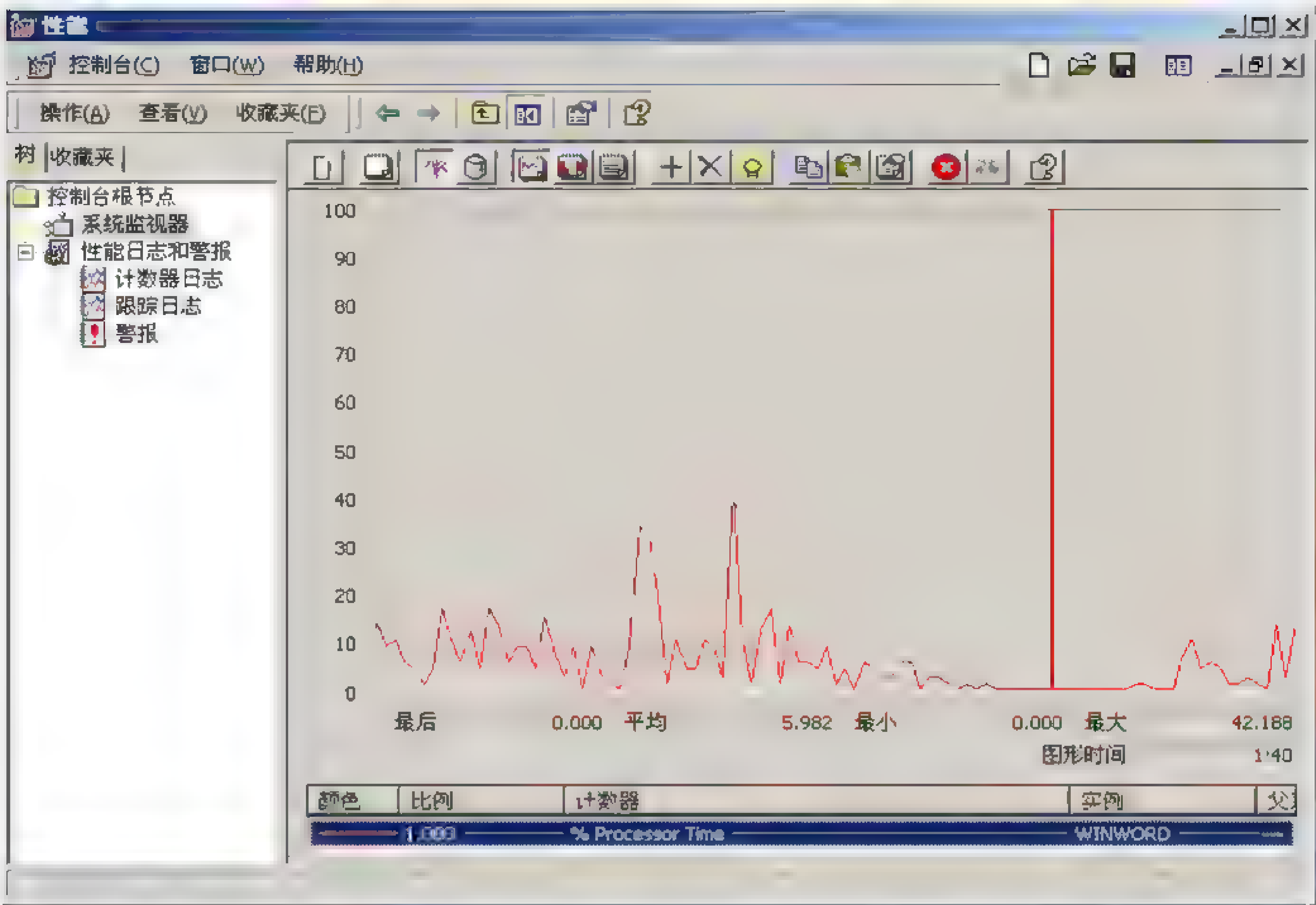


图 2-37 性能监视器



图 2-38 任务管理器

网络监视器监控网络在任何给定时间内通过网络的所有信息，并将数据帧复制到捕获缓冲区，然后在网络监视器的窗口上动态地显示。

网络监视器也允许远程捕获信息，这就要用到网络监视器代理。网络监视器代理能将统计数据送到本地计算机上，然后在本地网络监视器窗口上显示。网络监视器还具有对远程存取服务的局域网或广域网进行故障查找和排除的功能。

如果想实现捕获器在网络上的事件一被检测就立刻做出反应，可设计一个捕获器触发器。捕获器触发器执行指定的动作，例如，当网络监视器检测到网络上的一系列异常情况时启动一个可执行文件。

7. 输出基准报表

基准测量的结果是输出一个包含图表的基准报表，这些图表随时间的推移记录了每个网段的操作参数。除此之外，该报表还应该包括对异常情况和未来趋势的总结，对核心资源的利用率以及对报警阈值设置和监控的建议。

2.4.7　编写通信规范说明书

需求说明书是需求收集阶段的产物，而通信规范说明书也是通信分析阶段的主要产物；就如同需求说明书是产生通信规范分析的前提一样，通信规范说明书与需求说明书两者合起来为逻辑网络设计阶段提供了两个基本的输入文档资料。需求说明书描述的是新网络在将来要做什么，而通信规范说明书描述的是当前网络正在做什么。

通信规范说明书包含了估测的或实测的网络通信容量以及大量的统计表格，记录准确归纳和分析现存网络得到的结果，并根据该结果和需求说明书提出网络设计建议方案。

在正式编写通信规范说明书之前，要进行数据准备，包括通信分析阶段产生的大量未经处理的数据，如用户通信规范估测、通信规范测量、资源利用率统计数据等；通信规范说明书必须把所有的数据整理总结成一种能让网络设计者和管理人员都能看懂的文档。

一份好的通信规范说明书少不了网络图。几乎任何一种绘图软件都能用来生成这些图，但通常考虑选用专业的绘图软件（如 Visio），因为专业的绘图软件可以节省大量的时间。从长远利益来看，在一个提供好的度量和比例特征的应用软件中进行早期绘图，将能为以后的工作大大节省时间，从而提高工作效率。同时，所有的分析数据都应该妥善保存，就像保存未经加工的需求分析数据一样。当管理员们对读到的摘要产生怀疑时，可以查看保存的分析数据。

通信规范说明书记录了网络当前的状态，包括网络的配置、网络互联设备水平以及共享资源的利用率。通信规范说明书由下面主要内容组成。

- 执行情况概述。
- 分析阶段概述。

- 分析数据总结。
- 设计目标建议。
- 申请批准部分。
- 修改说明书。

1. 执行情况概述

在执行情况概述中，为了让网络管理人员清楚地了解进程的核心部分，此部分应该包含下列各项内容：

- 对项目的简单概述。
- 设计过程中各个阶段的清单。
- 项目各个阶段的状态，包括已完成的阶段和现在正进行的阶段。

2. 分析阶段概述

分析阶段主要描述如何收集信息和收集信息的时间，对于产生的信息，需要明确信息产生的方式，明确是估测信息还是实测信息。由于该文档是针对网络设计人员和网络管理员编写的，使用的语言应该是非专业人员能理解的描述性语言。

3. 分析数据总结

数据总结是通信规范说明书的核心，它同需求说明书中的数据总结一样重要。为准确展示当前网络的功能图，通信规范说明书应包括下述内容：

- 逻辑网络图。
- 通信流量估测（当前的和将来的）。
- 基准测量结果。
- CPU 利用率统计结果。

1）逻辑网络图

逻辑网络图是理解网络通信流量分布的重要内容。在逻辑网络图中，网络主要设备的位置、广域网范围的网络连接和主要的网络互联设备都应该清晰标识，如果条件允许，还应该标明工作组的边界和安全资源，如 Web 服务器或防火墙等。

2）通信流量估测

通信流量估测有助于分析全部通信流的方向和流量。可以用通信流量估测作为网络功能分析的依据，还应该对需要重点分析的内容进行标注，例如被过度使用的链路或设备等。建议使用表格的形式来表示估算的通信流量数据，或者在网络图上以标注的形式注明其流量和方向，通常情况下两种方法结合使用效果更好。

3）基准测量结果和 CPU 利用率统计结果

通信流量估测提供的是一种粗略的分析，而基准法测量和 CPU 利用率统计数据均侧重于用通信流量估测来暴露出需引起注意的地方。通过测试工具对通信流量和网络资源进行监控和分析，从而为设计提供依据。在复杂的升级网络中，应尽可能利用基准测量结果和 CPU 利用率等实测数据。

通信规范说明书中，应尽量通过图表形式向用户展现实测结果，在重点内容处进行

突出显示，并加入相应的说明文字，此外，应尽量避免使用技术术语，应该尽量使用非专业语言来解释专业的词汇。

4．设计目标建议

通信规范说明书应总结出网络设计的目标。为使新的网络满足需求分析，应在设计目标中说明哪些是必须被纠正的问题，哪些是必须添加的新功能。

根据需求说明书和通信规范说明书，提出的每一项建议都应该有依据，每一项建议都必须能解决一个问题，或满足一种业务需求。

总而言之，网络设计目标描述了新的网络设计应该达到的目标，以及为什么要达到这样的目标。

5．申请批准部分

在逻辑设计阶段之前，通信规范说明书必须已经通过了经理或核心成员组的批准和签字。该说明书的批准意味着管理部门认为通信规范说明书是真实的，同意逻辑设计列出的各项目标。

设计通信规范说明书时，注意提供一个可供每位经理和网络设计组组长签名的地方。

6．修改说明书

因为通信规范说明书是基于现有网络这一客观事实或者是对高可靠性的估测，所以管理部门对这些数据不可能有太大的争议。但是，在所有重要负责人完全达成一致之前，可能需要修改一些地方。

与处理需求说明书一样，不能通过修改数据或实验结果来满足新的设计目标。如果要修改或添加某个目标时，应该加上注释，解释为什么要修改或添加这个目标。

2.5　逻辑网络设计

2.5.1　逻辑设计过程概述

网络的逻辑结构设计，来自于用户需求中描述的网络行为、性能等要求，逻辑设计要根据网络用户的分类、分布，选择特定的技术，形成特定的网络结构，该网络结构大致描述了设备的互联及分布，但是不对具体的物理位置和运行环境进行确定。

逻辑设计过程主要由以下 4 个步骤组成：

- 确定逻辑设计目标。
- 网络服务评价。
- 技术选项评价。
- 进行技术决策。

2.5.1.1 逻辑网络设计目标

逻辑网络的设计目标主要来自于需求分析说明书中的内容，尤其是网络需求部分，由于这部分内容直接体现了网络管理部门和人员对网络设计的要求，因此需要重点考虑。一般情况下，逻辑网络设计的目标包括以下一些内容：

- 合适的应用运行环境：逻辑网络设计必须为应用系统提供环境，并可以保障用户能够顺利访问应用系统。
- 成熟而稳定的技术选型：在逻辑网络设计阶段，应该选择较为成熟稳定的技术，越是大型的项目，越要考虑技术的成熟度，以避免错误投入。
- 合理的网络结构：合理的网络结构不仅可以减少一次性投资，而且可以避免网络建设中出现各种复杂问题。
- 合适的运营成本：逻辑网络设计不仅仅决定了一次性投资，技术选型、网络结构也直接决定了运营维护等周期性投资。
- 逻辑网络的可扩充性能：网络设计必须具有较好的可扩充性，以便于满足用户增长、应用增长的需要，保证不会因为这些增长而导致网络重构。
- 逻辑网络的易用性：网络对于用户是透明的，网络设计必须保证用户操作的单纯性，过多的技术型限制会导致用户对网络的满意度降低。
- 逻辑网络的可管理性：对于网络管理员来说，网络必须提供高效的管理手段和途径，否则不仅会影响管理工作本身，也会直接影响用户。
- 逻辑网络的安全性：网络安全应提倡适度安全，对于大多数网络来说，既要保证用户的各种安全需求，也不能给用户带来太多限制；但是对于特殊的网络，也必须采用较为严密的网络安全措施。

2.5.1.2 需要关注的问题

1．设计要素

设计工作的要素主要包括：

- 用户需求。
- 设计限制。
- 现有网络。
- 设计目标。

逻辑设计过程，就是根据用户的需求，不违背设计限制，对现有网络进行改造或新建网络，最终达到设计目标的工作。

2．设计面临的冲突

网络设计工作中，设计目标是一个复杂的整体，由不同维度的子目标构成，这些子目标独立考虑时，存在较为明显的优劣关系，例如：

- 最低的安装成本。
- 最低的运行成本。
- 最高的运行性能。
- 最大的适应性。
- 最短的故障时间。
- 最大的可靠性。
- 最大的安全性。

这些子目标相互之间可能存在冲突，不存在一个网络设计方案，能够使得所有的子目标都达到最优。为了找到较为优秀的方案，来解决这些子目标的冲突，可以采用两种方法：第一种方式较为传统，由网络管理人员和设计人员一起，建立起这些子目标之间的优先级，尽量让优先级比较高的子目标达到较优；第二种方法，对每种子目标建立起权重，对子目标的取值范围进行量化，通过评判函数决定哪种方案最优，而子目标的权重关系直接体现了用户对不同目标的关心度。

3．成本与性能

成本与性能是最为常见的冲突目标，一般来说，网络设计方案的性能越高，也就意味着更高的成本，包括建设成本和运行成本。

设计方案时，所有不超过成本限制、满足用户要求的方案，都称为可行方案；设计人员只能从可行方案中依据用户对性能和成本的喜好进行选择。

4．款项支付

网络建设的成本分为一次性投资和周期性投资。

在初期建设过程中，如何合理规划一次性投资的支付，是比较关键的；过早支付费用，容易造成建设单位的风险，对于未按设计方案实施的情况，无法形成制约机制；过晚支付费用，容易造成承建单位的资金压力，导致项目实施质量等多方面的问题。较为合理的支付方式，必须是依据逻辑网络设计的特点，将网络工程划分为各个阶段，在每个阶段后实施验收，并支付相应的阶段费用，在工程建设完毕并试运行一段时间后，才能支付最后的质量保证费用。

运营维护等周期性费用的支付，也应考虑合理性，这主要体现在周期划分方式、支付方式等方面。

2.5.1.3　主要网络服务

网络设计人员应在依据网络提供的服务要求来选择特定的网络技术，不同的网络，其服务的要求不同，但是对于大多数网络来说，都存在着两个主要的网络服务——网络管理和网络安全，这些服务在设计阶段是必须考虑的。

1．网络管理服务

网络管理可以根据网络的特殊需要，将其划分为几个不同的大类，其中的重点内容

是网络故障诊断、网络的配置及重配置和网络监视。

1）网络故障诊断

网络故障诊断主要借助于网管软件、诊断软件和各种诊断工具。对于不同类型的网络和技术，需要的软件和工具是不同的；应在设计阶段就考虑到网络工程中各种诊断软件和工具的需要。

2）网络的配置及重配置

网络的配置及重配置是网络管理的另一个问题，各种网络设备都提供了多种配置方法，同时也提供了配置重新装载的功能。在设计阶段，考虑到网络设备的配置保存和更新需要，提供特定的配置工具以及配置管理工具，对于方便管理人员的工作是非常有必要的。

3）网络监视

网络监视的需求随着网络规模和复杂性的不同而不同，网络监视是为了预防灾难，使用监视服务来防止和监测网络的运行情况。

2．网络安全

网络安全系统是网络逻辑设计的固有部分，网络设计者可以采用以下步骤来进行安全设计。

1）明确需要安全保护的系统

首先要明确网络中需要重点保护的关键系统，通过该项工作，可以找出安全工作的重点，避免全面铺开而又无法面面俱到的局面。

2）确定潜在的网络弱点和漏洞

对于这些重点防护的系统，必须通过对这些系统的数据存储、协议传递、服务方式等的分析，找出可能存在的网络弱点和漏洞；在设计阶段，应依据工程经验对这些网络弱点和漏洞设计特定的防护措施；在实施阶段再根据实施效果进行调整。

3）尽量简化安全

安全设计要注意简化问题，不要盲目扩大安全技术和措施的重要性，适当时采用一些传统而有效、成本低廉的安全技术来提高安全性是非常有必要的。

4）安全制度

单纯的技术措施是无法保证网络的整体安全的，必须匹配相应的安全制度；逻辑设计阶段，尚不能制定完备的安全制度，但是对安全制度的大致性要求，包括培训、操作规范、保密制度等框架性要求是必须明确的。

2.5.1.4 技术评价

根据用户的需求设计逻辑网络，选择正确的网络技术比较关键，在进行选择时应考虑如下因素。

1．通信带宽

所选择的网络技术必须保证足够的带宽，能够为用户访问应用系统提供保障；在进行选择时，不能仅局限于现有的应用要求，还要考虑适当的带宽增长需求。

2．技术成熟性

所选择的网络技术必须是成熟稳定的技术，有些新的应用技术在尚没有大规模投入应用时，还存在着较多不确定因素，而这些不确定因素将会为网络建设带来很多不可估量的损失。虽然新技术的自身发展离不开工程应用，但是对于大型网络工程来说，项目本身不能成为新技术的试验田；因此，使用较为成熟、拥有较多案例的技术是明智的选择。

同时，在面对技术变革的特殊时期，可以采用试点的方式，缩小新技术的应用范围，规避技术风险，待技术成熟后再进行大规模应用。

3．连接服务类型

连接服务类型是逻辑设计时必须考虑的问题，传统的连接服务分为面相连接服务与非连接服务，逻辑设计需要在无连接和面向连接的协议之间进行权衡。

由于当前广泛应用的网络协议主要是 TCP/IP 协议族，其网络层协议是提供非连接服务的 IP 协议，因此选择连接服务类型，主要是对 IP 协议底层的承载协议进行选择。如果选择连接服务类型，则可以选择 ATM、SDH 等协议，如果选择非连接服务类型，则可以选择以太网等协议。不同的网络工程，对连接服务类型的需求不同，设计者不能仅局限于一种连接服务而进行设计。

4．可扩充性

网络设计者的设计依据是较为详细的需求分析，但是在选择网络技术时，不能仅考虑当前的需求，而忽视未来的发展；在大多数情况下，设计人员都会在设计中预留一定的冗余，无论是在带宽、通信容量、数据吞吐量、用户并发数等方面，网络实际需要和设计结果之间的比例应小于一个特定值以便于未来的发展；一般来说，这个值位于 70%～80%之间，在不同的工程中，可根据需要进行调整。

5．高投资产出

选择网络技术的最关键一条，不是技术的扩展性、高性能性，也不是成本最低等概念，决定设计和网络管理人员采用某种技术的最关键的一点是技术的投入产出比，尤其是一些借助于网络来实现营运的工程，只有通过投入产出分析，才能最后决定技术的使用。

2.5.1.5　具体工作内容

逻辑网络设计工作主要包括如下的内容：

- 网络结构的设计。
- 物理层技术选择。

- 局域网技术选择与应用。
- 广域网技术选择与应用。
- 地址设计和命名模型。
- 路由选择协议。
- 网络管理。
- 网络安全。
- 逻辑网络设计文档。

2.5.2 网络结构设计

传统意义上的网络拓扑，是将网络中的设备和节点描述成点，将网络线路和链路描述成线，随着网络的不断发展，单纯的网络拓扑结构已经无法全面描述网络；因此，在逻辑网络设计中，网络结构的概念正在取代网络拓扑结构的概念，成为网络设计的框架。

网络结构是对网络进行逻辑抽象，描述网络中主要连接设备和网络计算机节点分布而形成的网络主体框架，网络结构与网络拓扑结构的最大区别在于：网络拓扑结构中，只有点和线，不会出现任何的设备和计算机节点；网络结构主要是描述连接设备和计算机节点的连接关系。

由于当前的网络工程主要由局域网和实现局域网互联的广域网构成，因此可以将网络工程中的网络结构设计分成局域网结构和广域网结构两个设计部分内容，其中局域网结构主要讨论数据链路层的设备互连方式，广域网结构主要讨论网络层的设备互连方式。

2.5.2.1 局域网结构

当前的局域网络与传统意义上的局域网络已经发生了很多变化，传统意义上的局域网络只具备二层通信功能，而现代意义上的局域网络不仅具有二层通信功能，同时具有三层甚至多层通信的功能。现代局域网络，从某种意义上说，被称为园区网络更为合适。

以下是在进行局域网络设计时，常见的局域网结构。

1．核心局域网结构

单核心局域网结构主要由一台核心二层或三层交换设备构建局域网络的核心，通过多台接入交换机接入计算机节点，该网络一般通过与核心交换机互连的路由设备（路由器或防火墙）接入广域网中。

典型的单核心结构如图2-39所示。

单核心结构分析如下：

- 核心交换设备在实现上多采用二层、三层交换机或多层交换机。
- 如采用三层或多层设备，可以划分成多个 VLAN，VLAN 内只进行数据链路层帧转发。

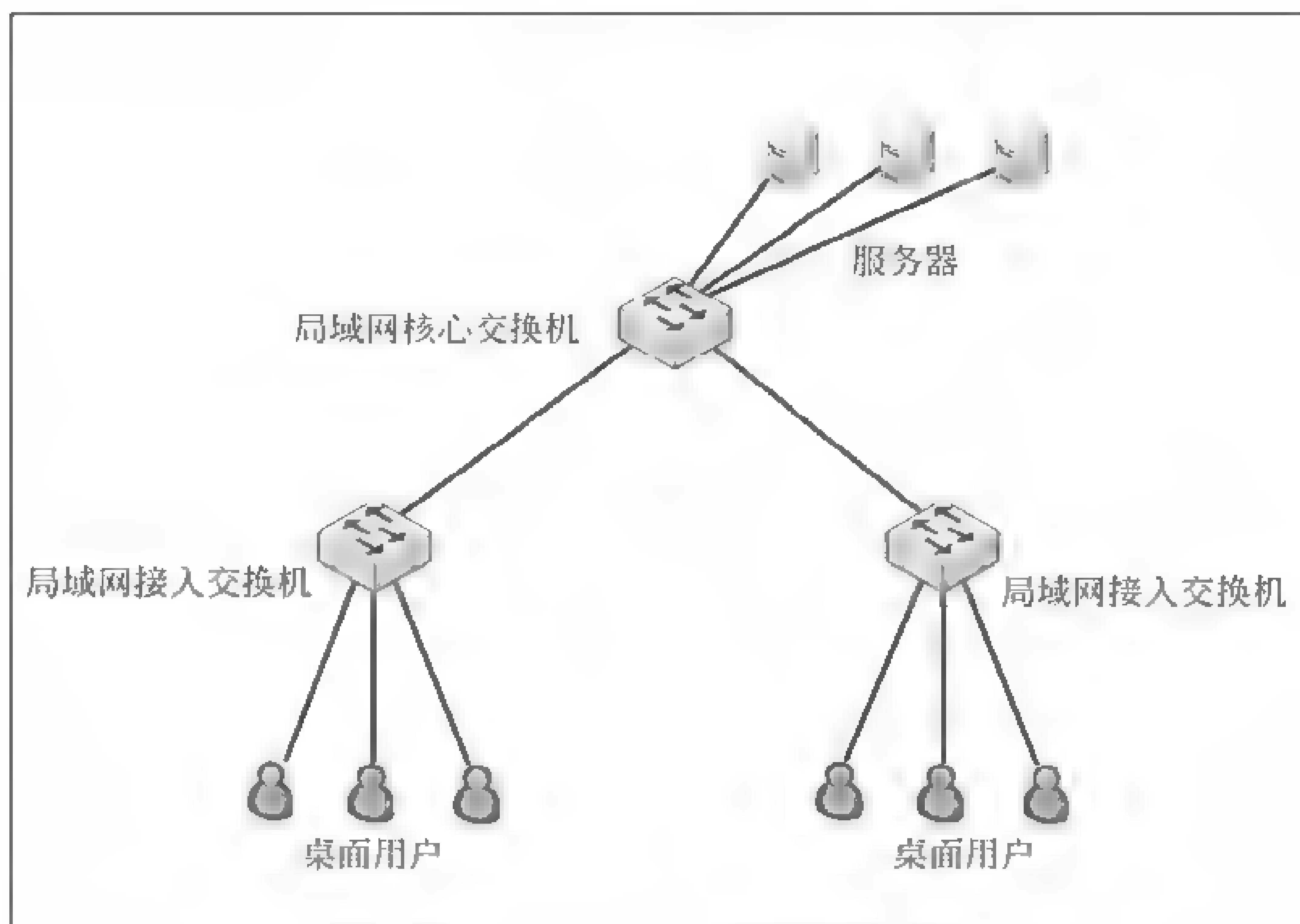


图 2-39　单核心局域网结构

- 网络内各 VLAN 之间访问需要经过核心交换设备，并且只能通过网络层数据包转发方式实现。
- 网络中除核心交换设备之外，不存在其他的带三层路由功能的设备。
- 核心交换设备与各 VLAN 设备可以采用 10M/100M/1000M 以太网连接。
- 节省设备投资。
- 网络结构简单。
- 部门局域网络访问核心局域网以及相互之间访问效率高。
- 在核心交换设备端口富余前提下，部门网络接入较为方便。
- 网络地理范围小，要求部门网络分布比较紧凑。
- 核心交换机是网络的故障单点，容易导致整网失效。
- 网络扩展能力有限。
- 对核心交换设备的端口密度要求较高。
- 除非规模较小的网络，否则推荐桌面用户不直接与核心交换设备相连，也就是核心交换机与用户计算机之间应存在接入交换机。

2．双核心局域网结构

双核心结构主要由两台核心交换设备构建局域网核心，该网络一般也是通过与核心交换机互连的路由设备接入广域网，并且路由器与两台核心交换设备之间都存在物理链路。

典型的双核心结构如图2-40所示。

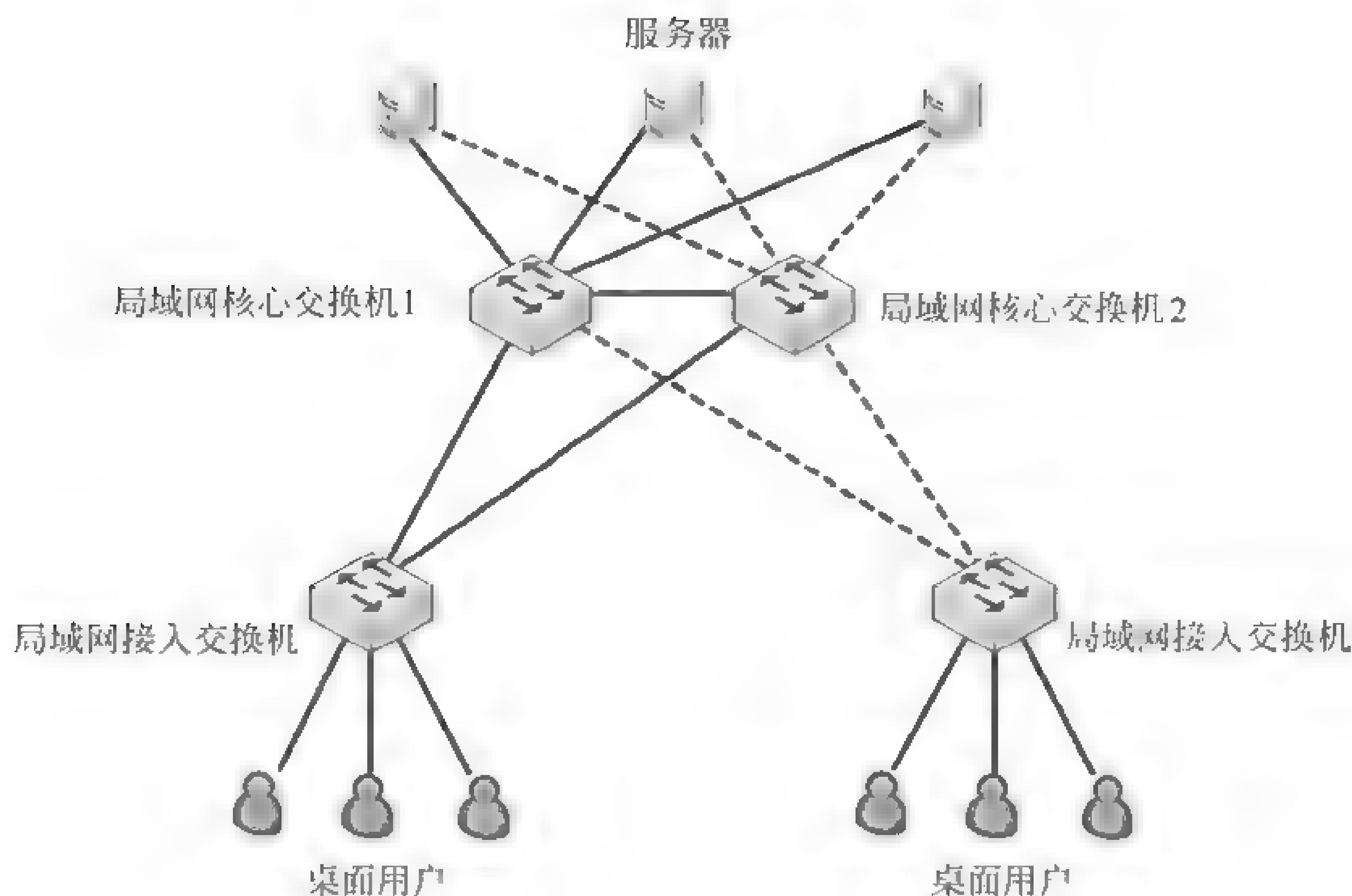


图 2-40 双核心局域网结构

双核心结构分析如下：

- 核心交换设备在实现上多采用三层交换机或多层交换机。
- 网络内各 VLAN 之间访问需要经过两台核心交换设备中的一台。
- 网络中除核心交换设备之外，不存在其他的具备路由功能的设备。
- 核心交换设备之间运行特定的网关保护或负载均衡协议，例如 HSRP、VRRP、GLBP 等。
- 核心交换设备与各 VLAN 设备间可以采用 10M/100M/1000M 以太网连接。
- 网络拓扑结构可靠。
- 路由层面可以实现无缝热切换。
- 部门局域网络访问核心局域网以及相互之间多条路径选择可靠性更高。
- 在核心交换设备端口富余前提下，部门网络接入较为方便。
- 设备投资比单核心高。
- 对核心路由设备的端口密度要求较高。
- 核心交换设备和桌面计算机之间，存在接入交换设备，接入交换设备同时和双核心存在物理连接。
- 所有服务器都直接同时连接至两台核心交换机，借助于网关保护协议，实现桌面用户对服务器的高速访问。

3．环型局域网结构

环型局域网结构由多台核心三层设备连接成双 RPR 动态弹性分组环，构建整个局域

网络的核心，该网络通过与环上交换设备互连的路由设备接入广域网络。

典型的环型结构如图2-41所示。

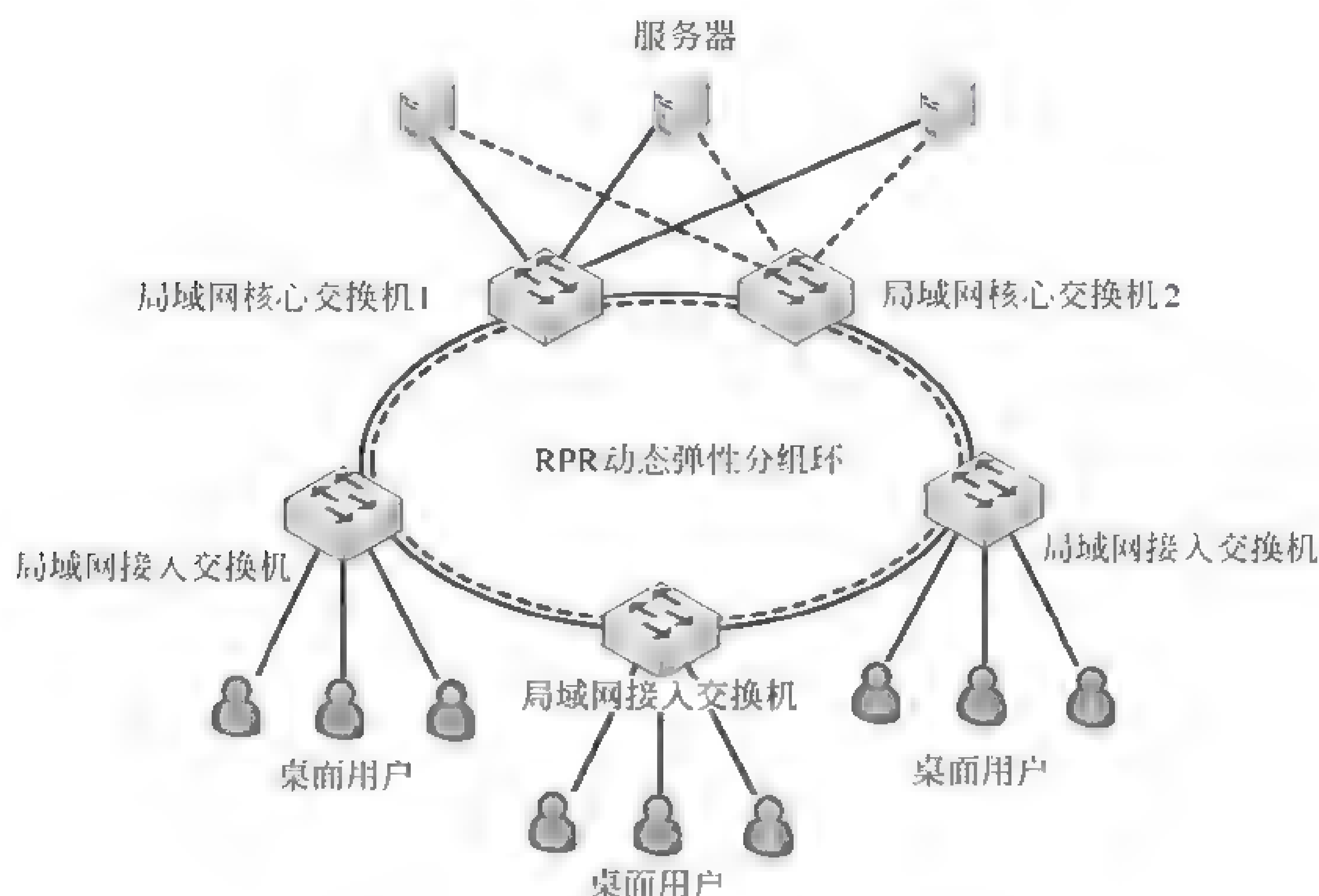


图 2-41　环型局域网结构

环型结构分析如下：

- 核心交换设备在实现上多采用三层交换机或多层交换机。
- 网络内各 VLAN 之间访问需要经过 RPR 环。
- RPR 技术能提供 MAC 层的 50ms 自愈时间，能提供多等级、可靠的 QoS 服务。
- RPR 有自愈保护功能，节省光纤资源。
- RPR 协议中没有提及相交环、相切环等组网结构，当利用 RPR 组建大型城域网时，多环之间只能利用业务接口进行互通，不能实现网络的直接互通，因此它的组网能力相对 SDH、MSTP 较弱。
- 由两根反向光纤组成环型拓扑结构。其中一根顺时针，一根逆时针，节点在环上可从两个方向到达另一节点。每根光纤可以同时用来传输数据和同向控制信号，RPR 环双向可用。
- 利用空间重用技术实现的空间重用，使环上的带宽得到更为有效的利用。RPR 技术具有空间复用、环自愈保护、自动拓扑识别、多等级 QoS 服务、带宽公平机制和拥塞控制机制、物理层介质独立等技术特点。
- 设备投资比单核心高。
- 核心路由冗余设计实施难度较高，容易形成路由环路。

4．层次局域网结构

层次结构主要定义了根据功能要求不同将局域网络划分层次构建的方式，从功能上定义为核心层、会聚层、接入层。层次局域网一般通过与核心层设备互连的路由设备接入广域网络。

典型的层次结构如图2-42所示。

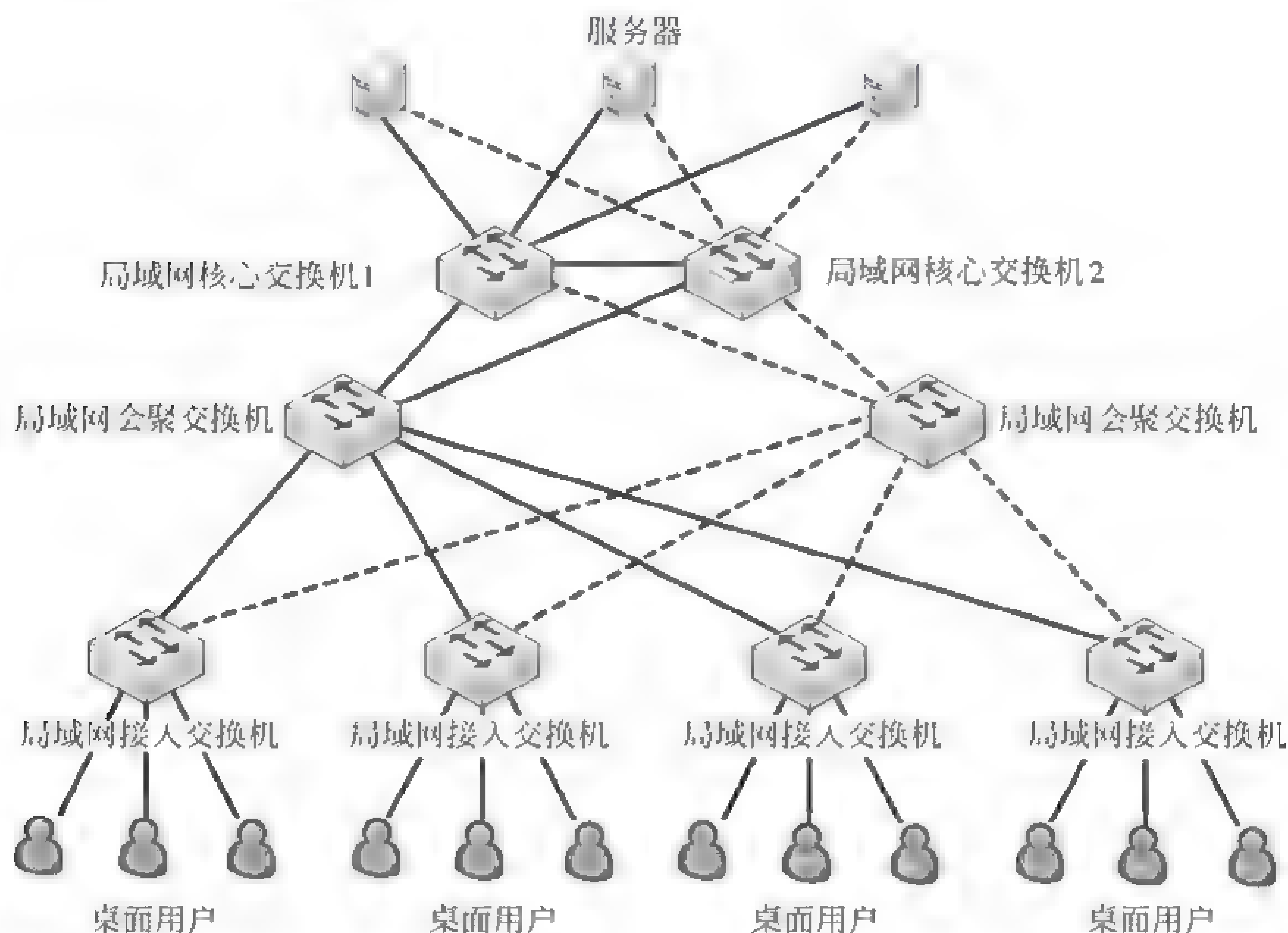


图2-42 层次局域网结构

层次结构分析如下：

- 核心层实现高速数据转发。
- 会聚层实现丰富的接口和接入层之间的互访控制。
- 接入层实现用户接入。
- 网络拓扑结构故障定位可分级便于维护。
- 网络功能清晰有利发挥设备最大效率。
- 网络拓扑利于扩展。

2.5.2.2 广域网结构

在大多数网络工程中，利用广域网实现多个局域网络的互联，形成整个网络的网络结构。

在以下各广域网结构分析中，没有在局域网与广域网之间定义其他路由设备，但是

在设计与实施时，可以根据需要添加特定的接入路由器或防火墙设备；在局域网络规模较为复杂时，可以添加接入路由器；在局域网络有安全需要时，可以添加防火墙。

1．单核心广域网结构

单核心结构主要由一台核心路由设备互联各局域网络。

典型的单核心结构如图2-43所示。

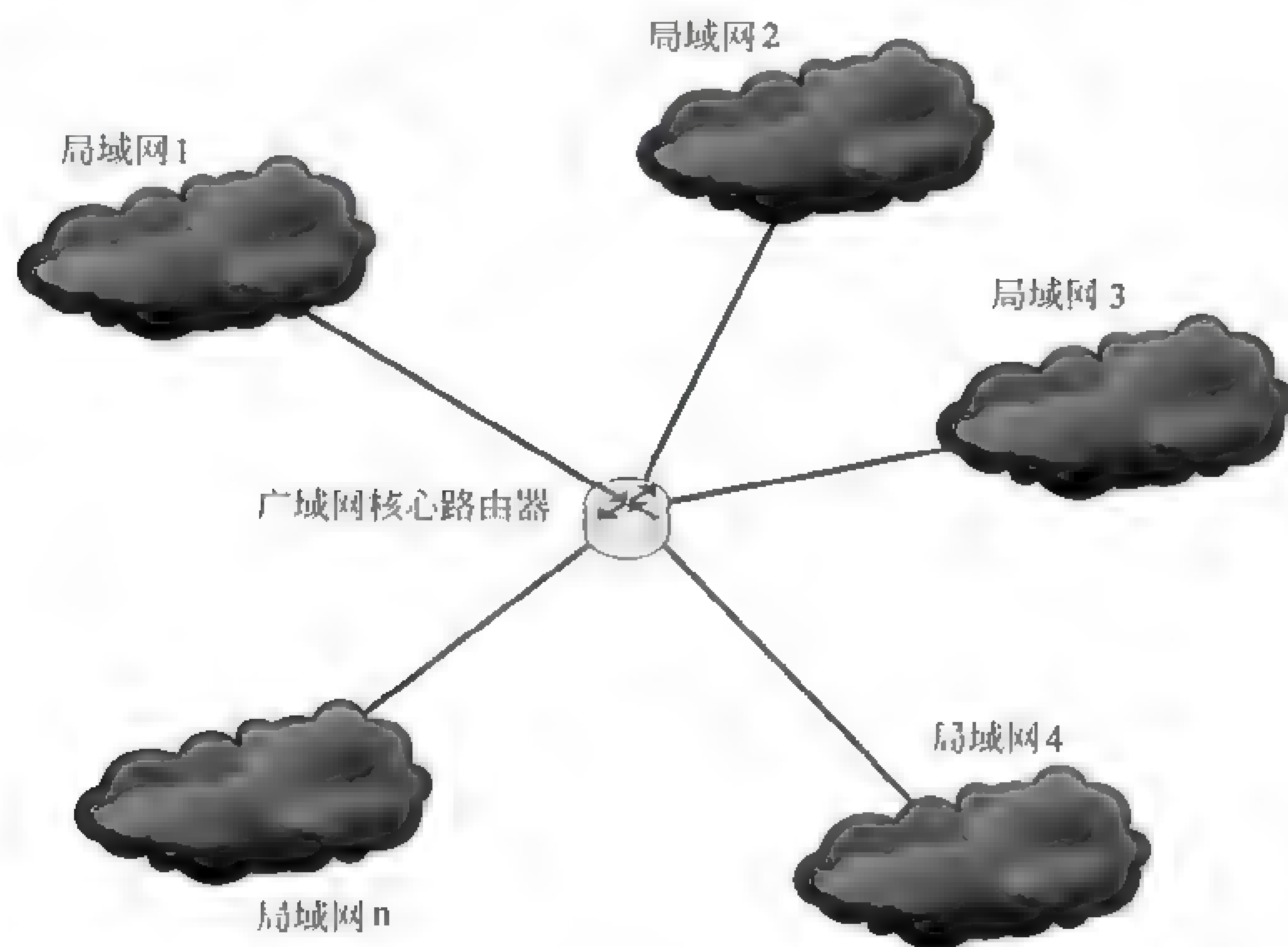


图 2-43　单核心广域网结构

单核心结构分析如下：

- 核心路由设备在实现上多采用三层交换机或多层交换机。
- 网络内各局域网络之间访问需要经过核心路由设备。
- 网络中除核心路由设备之外，不存在其他路由设备。
- 各部门局域网至核心路由设备之间不采用点对点线路，而采用广播线路，路由设备与部门局域网络互联的接口属于该局域网。
- 核心路由设备与各局域网可以采用 10M/100M/1000M 以太网连接。
- 节省设备投资。
- 网络结构简单。
- 部门局域网络访问核心局域网以及相互之间访问效率高。
- 在核心路由设备端口富余前提下，部门网络接入较为方便。
- 核心路由器是网络的故障单点，容易导致整网失效。
- 网络扩展能力有限。
- 对核心路由设备的端口密度要求较高。

2．双核心广域网结构

双核心结构主要由两台核心路由设备构建框架，并互联各局域网。

典型的双核心结构如图2-44所示。

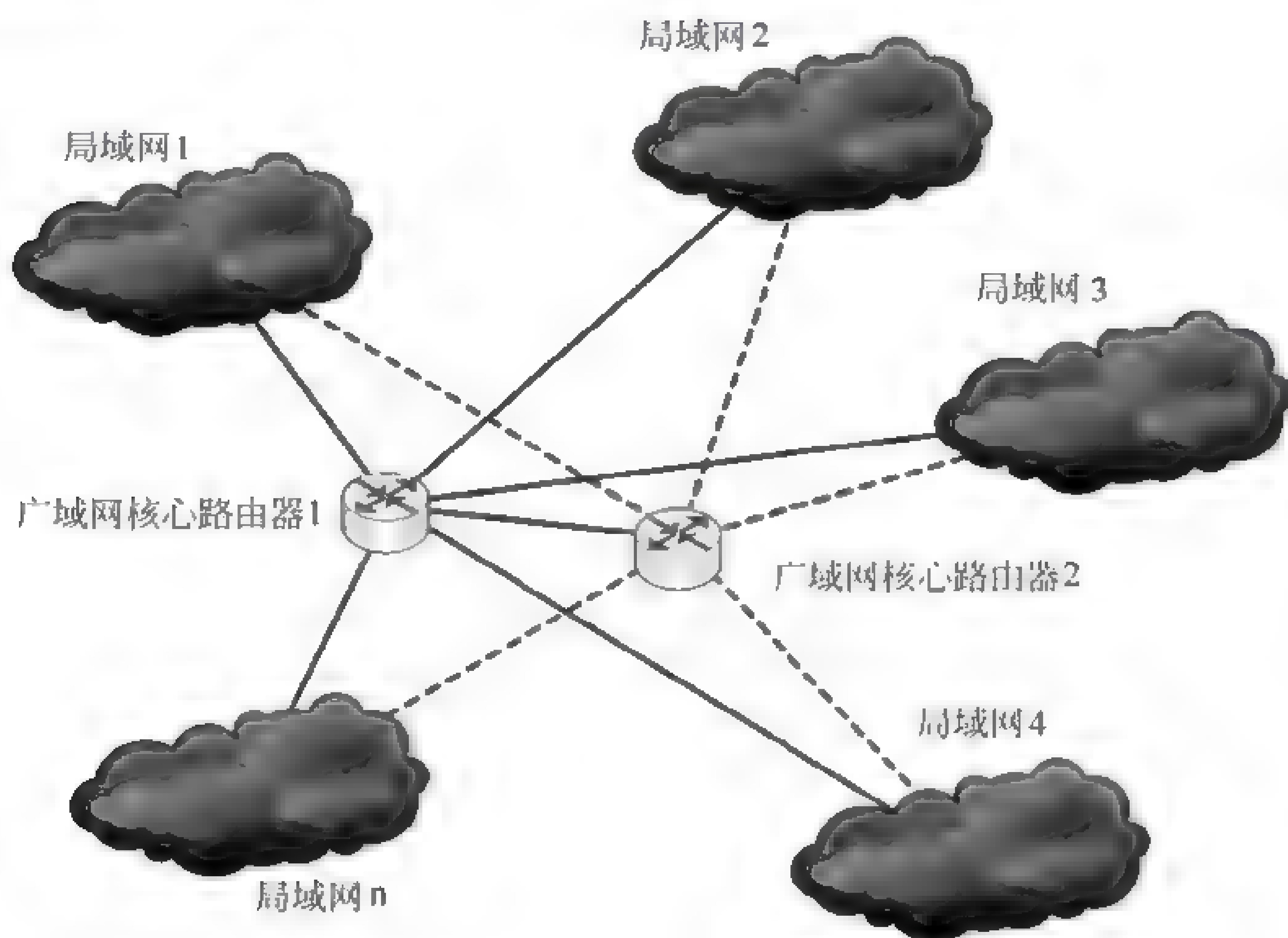


图 2-44 双核心广域网结构

双核心结构分析如下：

- 核心路由设备在实现上多采用三层交换机或多层交换机。
- 网络内各局域网络之间访问需要经过两台核心路由设备中的一台。
- 网络中除核心路由设备之外，不存在其他的路由设备。
- 核心路由设备之间运行特定的网关保护或负载均衡协议，例如 HSRP、VRRP、GLBP 等。
- 核心路由设备与各局域网可以采用 10M/100M/1000M 以太网连接。
- 网络拓扑结构可靠。
- 路由层面可以实现无缝热切换。
- 部门局域网络访问核心局域网以及相互之间多条路径选择可靠性更高。
- 在核心路由设备端口富余前提下，部门网络接入较为方便。
- 设备投资比单核心高。
- 核心路由器路由冗余设计实施难度较高，容易形成路由环路。
- 对核心路由设备的端口密度要求较高。

3．环型广域网结构

环型结构主要定义了由三台以上核心路由设备构成路由环路，连接各局域网并构建

广域网的方式，在环型广域网结构中，任意核心路由器都和其他两台路由设备之间有连接。

典型的环型结构如图2-45所示。

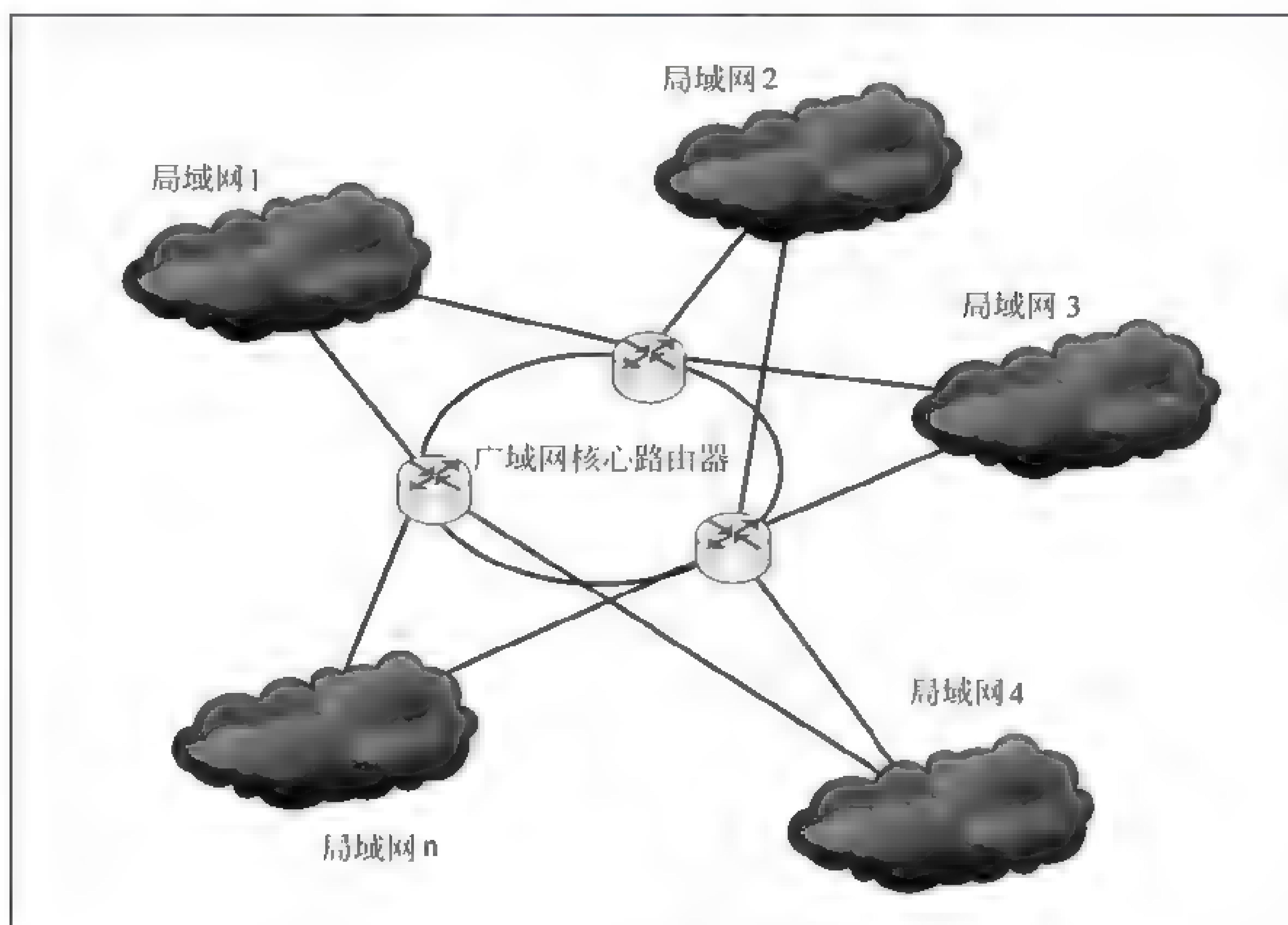


图 2-45　环型广域网结构

环型结构分析如下：

- 核心路由设备在实现上多采用三层交换机或多层交换机。
- 网络内各局域网络之间访问需要经过核心路由设备构成的环。
- 网络中除核心路由设备之外，不存在其他的路由设备。
- 核心路由设备之间运行特定的网关保护或负载均衡协议，例如 HSRP、VRRP、GLBP 等；或具备环路控制功能协议，例如 OSPF、RIP 等。
- 核心路由设备与各局域网可以采用 10M/100M/1000M 以太网连接。
- 网络拓扑结构可靠。
- 路由层面可以实现无缝热切换。
- 部门局域网络访问核心局域网以及相互之间多条路径选择可靠性更高。
- 在核心路由设备端口富余前提下，部门网络接入较为方便。
- 设备投资比双核心高。
- 核心路由器路由冗余设计实施难度较高，容易形成路由环路。
- 对核心路由设备的端口密度要求较高。
- 环型拓扑占用较多的端口。

4．半冗余广域网结构

半冗余结构主要定义了由多台核心路由设备连接各局域网并构建广域网络的方式，在半冗余结构中，任意核心路由器存在至少两条以上连接至其他路由设备；如果核心路由器和任何其他路由器都有连接，就是半冗余结构的特例——全冗余广域网结构。

典型的半冗余结构如图2-46所示。

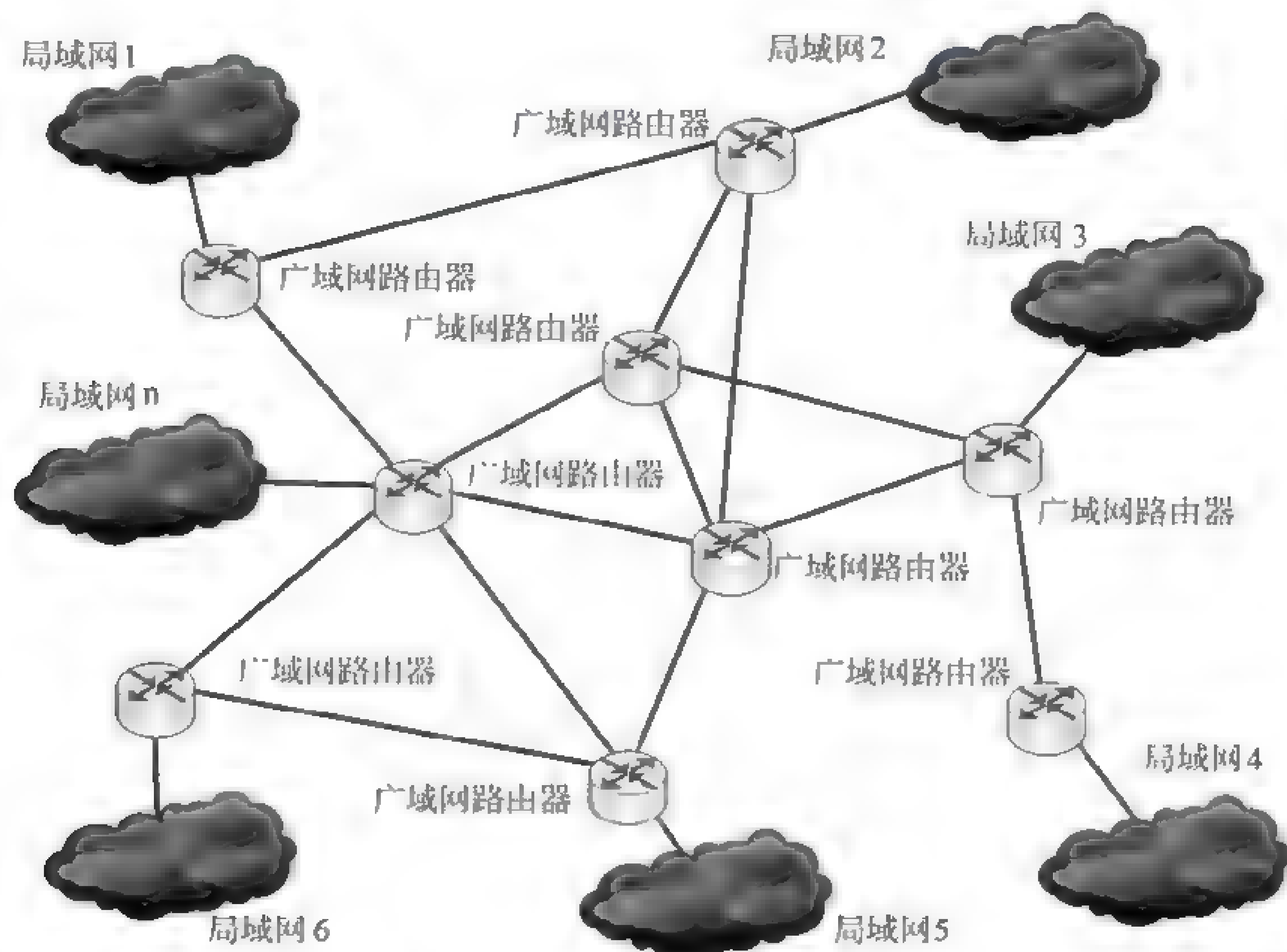


图2-46 半冗余广域网结构

半冗余结构分析如下：

- 半冗余网络结构灵活、方便扩展。
- 部分网络可以采用特定的网关保护或负载均衡协议，例如HSRP、VRRP、GLBP等；或具备环路控制功能协议，例如OSPF、RIP等。
- 网络拓扑结构相对可靠，呈网状。
- 路由层面路径选择比较灵活可以有多条备选路径。
- 部门局域网络访问核心局域网以及相互之间多条路径选择，可靠性高。
- 网络结构零散管理和故障排除不太方便。
- 该网络结构适合部署OSPF等链路状态路由协议。

5．对等子域广域网结构

对等子域结构是指通过将广域网的路由器划分成两个独立的子域，每个子域内路由

器采用半冗余方式互连。对等子域结构中，两个子域间通过一条或多条链路互连，对等子域结构中任何路由器都可以接入局域网络。

典型的对等子域结构如图2-47所示。

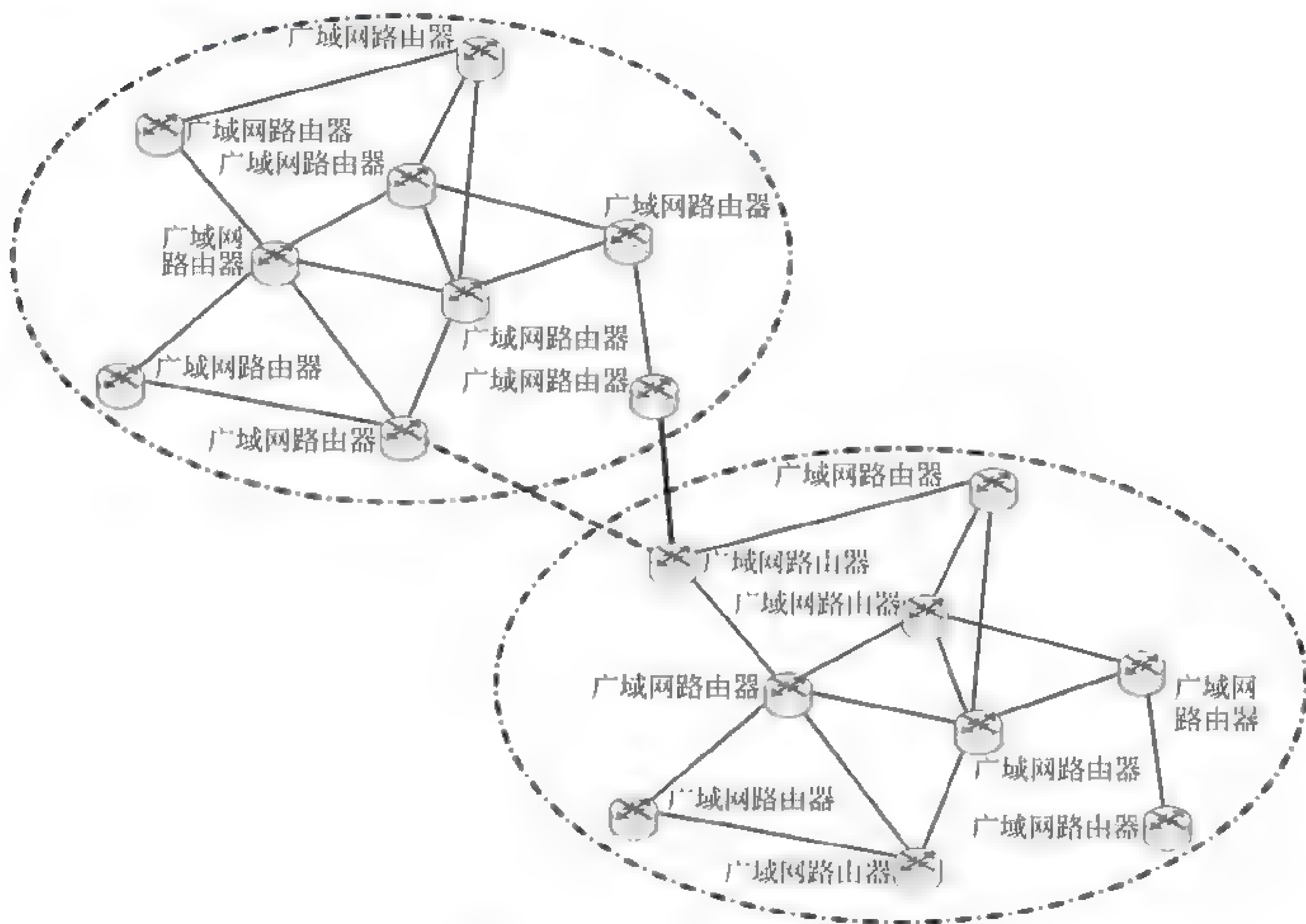


图 2-47　对等子域广域网结构

对等子域结构分析如下：

- 对等子域之间的互访以对等子域之间的互连线路为主。
- 对等子域之间可以做到路由汇总或明细路由条目匹配，路由控制灵活。
- 子域间链路带宽应高于子域内链路带宽。
- 域间路由冗余设计实施难度较高，容易形成路由环路或发布非法路由的问题。
- 对用于域互访的域边界路由设备的路由性能要求较高。
- 路由协议的选择主要以动态路由为主。
- 对等子域适合于广域网络可以明显划分为两个区域，并且区域内部访问较为独立的情况。

6．层次子域广域网结构

层次子域结构将大型广域网路由设备划分为多个较为独立的子域，每个子域内路由器采用半冗余方式互连。层次子域结构中，多个子域之间存在层次关系，高层子域连接

多个低层子域。层次子域结构中任何路由器都可以接入局域网络。

典型的层次子域结构如图2-48所示。

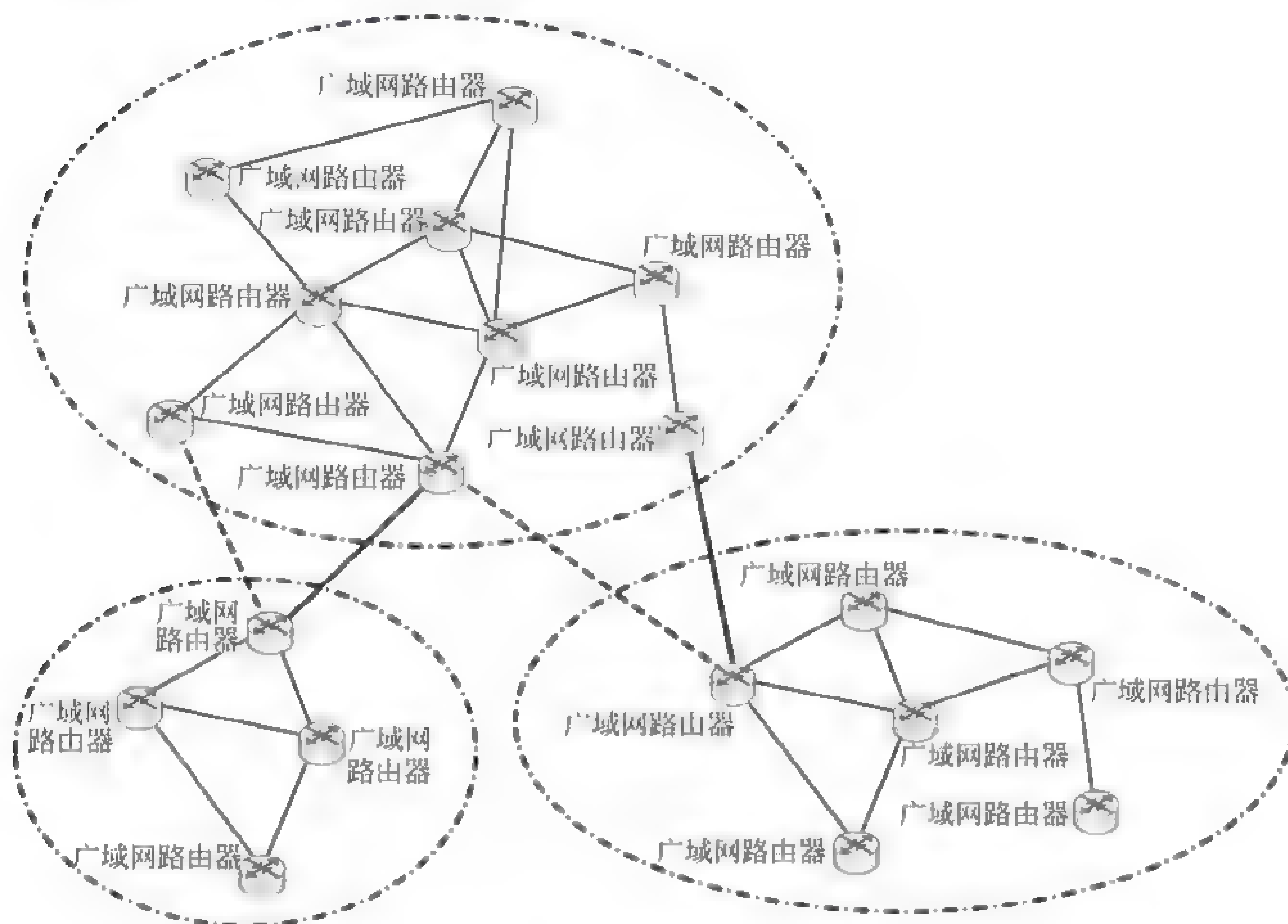


图 2-48　层次子域广域网结构

层次子域结构分析如下：

- 低层子域之间的互访应通过高层子域完成。
- 层次子域结构具有较好的扩展性。
- 子域间链路带宽应高于子域内链路带宽。
- 域间路由冗余设计实施难度较高，容易形成路由环路或发布非法路由的问题。
- 对用于域互访的域边界路由设备的路由性能要求较高。
- 路由协议的选择主要以动态路由为主，尤其适用于 OSPF 协议。
- 层次子域结构与上层外网互联，主要借助于高层子域完成；与下层外网互联，主要借助于低层子域完成。

2.5.2.3　层次化网络设计模型

1．层次化网络设计模型

层次化网络设计模型可以帮助设计者按层次设计网络结构，并对不同层次赋予特定

的功能，为不同层次选择正确的设备和系统。一个典型的层次化网络结构包括以下特征：

- 由经过可用性和性能优化的高端路由器和交换机组成的核心层。
- 由用于实现策略的路由器和交换机构成的会聚层。
- 由用于连接用户的低端交换机等构成的接入层。

在上述的网络结构介绍中，层次局域网结构和层次子域广域网结构就是层次化网络设计模型分别在局域网和广域网设计中的应用；随着用户不断增多，网络复杂度也不断增大，层次化网络设计模型也成为位于网络主流的园区网络的经典模型。

采用层次化网络设计模型进行设计工作，具有如下的优点：

（1）使用层次化模型可以使网络成本降到最低，通过在不同层次设计特定的网络互联设备，可以避免为各层中不必要的特性而花费过多的资金；层次化模型可以在不同层次进行更精细的容量规划，从而减少贷款浪费；同时，层次化模型可以使得网络管理产生层次性，不同层次的网络运行管理人员的工作职责也不同，培训规模和管理成本也不同，从而减少控制管理成本。

（2）层次化设计模型在设计中，可以采用不同层次上的模块化，模块就是层次上的设备及连接集合，这使得每个设计元素简化并易于理解，并且网络层次间交界点也很容易识别，使得故障隔离得到提高，保证了网络的稳定性。

（3）层次化设计使网络的改变变得更加容易，当网络中的一个网元需要改变时，升级的成本限制在整个网络中很小的一个子集中，对网络的整体影响达到最小。

2．三层层次化模型

层次化模型中最为经典的是三层层次化模型，该模型允许在三个练习的路由或交换层次上实现流量会聚和过滤，这使得三层层次化模型的规模可以从中小型公司的网络扩充到大型的国际互联网络。

三层层次化模型主要将网络划分为核心层、会聚层和接入层，每一层都有着特定的作用；核心层提供不同区域或者下层的高速连接和最优传送路径；会聚层将网络业务连接到接入层，并且实施与安全、流量负载和路由相关的策略；接入层为局域网接入广域网或者终端用户访问网络提供接入。

1）核心层设计要点

核心层是互联网络的高速骨干，由于其重要性，因此在设计中应该采用冗余组件设计，使其具备高可靠性，能快速适应变化。

在设计核心层设备的功能时，应尽量避免使用数据包过滤、策略路由等降低数据包转发处理的特性，以优化核心层获得低延迟和良好的可管理性。

核心层应具有有限的和一致的范围，如果核心层覆盖的范围过大，连接的设备过多，必然引起网络的复杂度加大，导致网络管理性降低；同时如果核心层覆盖的范围不一致，必然导致大量处理不一致情况的功能都在核心层网络设备中实现，会降低核心网络设备的性能。

对于那些需要连接因特网和外部网络的网络工程来说，核心层应包括一条或多条连接到外部网络的连接，这样可以实现外部连接的可管理性和高效性。

2）会聚层设计要点

会聚层是核心层和接入层的分界点，应尽量将出于安全性原因对资源访问的控制、出于性能原因对通过核心层流量的控制等，都在会聚层实施。

为保证层次化的特性，会聚层应该向核心层隐藏接入层的详细信息，例如，不管接入层划分了多少个子网，会聚层向核心层路由器进行路由宣告时，仅会宣告多个子网地址会聚而形成的一个网络。另外，会聚层也会对接入层屏蔽网络其他部分的信息，例如会聚层路由器可以不向接入路由器宣告其他网络部分的路由，而仅仅向接入设备宣告自己是默认路由。

为了保证核心层连接运行不同协议的区域，各种协议的转换都应在会聚层完成；例如局域网络中，运行了传统以太网和弹性分组环网的不同会聚区域；例如运行了不同路由算法的区域，可以借助于会聚层设备完成路由的汇总和重新发布。

3）接入层设计要点

接入层为用户提供了在本地网段访问应用系统的能力，接入层要解决相邻用户之间的互访需要，并且为这些访问提供足够的带宽。

接入层还应当适当负责一些用户管理功能，包括地址认证、用户认证、计费管理等内容。

接入层还负责一些用户信息收集工作，例如用户的 IP 地址、MAC 地址、访问日志等信息。

3．层次化设计的原则

层次化网络设计应该遵循一些简单的原则，这些原则可以保证设计出来的网络更加具有层次的特性：

（1）在设计时，设计者应该尽量控制层次化的程度，一般情况下，由核心层、会聚层、接入层三个层次就足够了，过多的层次会导致整体网络性能的下降，并且会提高网络的延迟，同时也方便网络故障排查和文档编写。

（2）在接入层应当保持对网络结构的严格控制，接入层的用户总是为了获得更大的外部网络访问带宽，而随意申请其他的渠道访问外部网络，这是不允许的。

（3）为了保证网络的层次性，不能在设计中随意加入额外连接，额外连接是指打破层次性，在不相邻层次间的连接，这些连接会导致网络中的各种问题，例如缺乏会聚层的访问控制和数据包过滤等。

（4）在进行设计时，应当首先设计接入层，根据流量负载、流量和行为的分析，对上层进行更精细的容量规划，再依次完成各上层的设计。

（5）除去接入层的其他层次，应尽量采用模块化方式，每个层次由多个模块或者设备集合构成，每个模块间的边界应非常清晰。

2.5.2.4　网络冗余设计

网络冗余设计允许通过设置双重网络元素来满足网络的可用性需求，冗余避免了网络的单点失效，其目标是重复设置网络组件，以避免单个组件的失效而导致应用失效。这些组件可以是一台核心路由器、交换机，可以是两台设备间的一条链路，可以是一个广域网连接，可以是电源、风扇、设备引擎等设备上的模块。对于某些大型网络来说，为了确保网络中的信息安全，在独立的数据中心之外，还设置了冗余的容灾备份中心，以保证数据备份或者应用在故障下的切换。

在网络冗余设计中，对于通信线路常见的设计目标主要有两个：一个是备用路径，另外一个是负载分担。

1．备用路径

备用路径主要是为了提高网络的可用性。当一条路径或者多条路径出现故障时，为了保障网络的连通，网络中必须存在冗余的备用路径；备用路径由路由器、交换机等设备之间的独立备用链路构成，一般情况下，备用路径仅仅在主路径失效时投入使用。

设计备用路径时主要考虑以下因素：

（1）备用路径的带宽。备用路径带宽的依据，主要是网络中重要区域、重要应用的带宽需要，设计人员要根据主路径失效后，哪些网络流量是不能中断来形成备用路径的最小带宽需求。

（2）切换时间。切换时间指从主路径故障到备用路径投入使用的时间，切换时间主要取决于用户对应用系统中断服务时间的容忍度。

（3）非对称。备用路径的带宽比主路径的带宽小是正常的设计方法，由于备用路径大多数情况下并不投入使用，过大的带宽容易造成浪费。

（4）自动切换。设计备用路径时，应尽量采用自动切换方式，避免使用手工切换。

（5）测试。备用路径由于长期不投入使用，对线路、设备上存在的问题，不容易发现，应设计定期的测试方法，以便于及时发现问题。

2．负载分担

负载分担是通过冗余的形式来提高网络的性能，是对备用路径方式的扩充。负载分担是通过并行链路提供流量分担来提高性能，其主要的实现方法是利用两个或多个网络接口和路径来同时传递流量。

关于负载分担，设计时主要考虑以下因素：

（1）网络中存在备用路径、备用链路时，就可以考虑加入负载分担设计。

（2）对于主路径、备用路径都相同的情况，可以实施负载分担的特例——负载均衡，也就是多条路径上的流量是均衡的。

（3）对于主路径、备用路径不相同的情况，可以采用策略路由机制，让一部分应用的流量分摊到备用路径上。

（4）在路由算法的设计上，大多数设备制造厂商实现的路由算法，都能够在相同带宽的路径上实现负载均衡，甚至于部分特殊的路由算法，例如 IGRP 和增强 IERP 中，可以根据主路径和备用路径的带宽比例实现负载分担。

2.5.3 物理层技术选择

在确定了大致的网络结构之后，需要对网络中物理层技术进行选择，这些技术选择内容包括缆线类型、选用网卡等。

选择物理层技术时，不能仅局限于当前的需要，还要考虑到网络升级所带来的需求。

2.5.3.1 技术选择原则

物理层技术的选择依据主要来自于需求分析说明书和通信规范说明书，这些说明书中已经明确了带宽等通信参数的要求。

以下是对满足说明书要求的技术进行选择时的一些通用原则。

1．可扩展性与可伸缩性

选择底层技术时，一定要考虑扩展性，否则将导致大量物理层设备的替换。例如尽管需求说明书中提出了带宽的要求小于 10Mbps，但是在设计时，仍可以采用第 5 类非屏蔽线和百兆网卡，以避免当应用升级后导致的网络重新布线以及网卡淘汰，这样当整个网络升级至快速以太网时，仅需要更换交换设备。

2．可靠性、可用性和可恢复性

物理层的可靠性、可用性和可恢复性主要来自于应用的需求，如果物理层不稳定，必然导致承载的应用出现故障，应尽量选择较为稳定、可靠的物理层技术。例如，在实现远程用户的接入时，不选择基于模拟信号调制的语音拨号接入方式，而是选择基于数字信号编码的 ISDN 或者 ADSL 方式。例如，在专网建设中，如果用户存在变动或升级带宽的需求，则不能采用带宽固定的 SDH 信道，而是采用可以动态变化带宽的 ATM PVC 方式。

3．安全性

物理层的不安全因素是指未经授权而非法访问网络介质，通常的做法是利用监听线缆来监视传输。不同的物理介质有不同的内在安全特征，所以客户的安全决定了对物理层设备的选择。例如，针对一些特殊部门的接入，采用光缆以避免信号窃听；或者是采用屏蔽线缆替代非屏蔽线缆。

4．节约与成本

节约成本也是需要着重考虑的一个问题。例如，在经济上考虑是否使用现存的线缆或网卡，从成本上考虑是需要内部安装人员还是专业的承包人。

2.5.3.2 物理介质和网卡的考虑

对有关物理层的需求了解清楚后，就可以选择物理介质和网卡了。

1．物理介质

物理介质包括有线介质和无线介质，表 2-14 是对各种介质的比较，直接体现了在设计中的应用范围，设计人员应根据需求和表 2-14 的对应选择大致的物理介质类型。

表 2-14　物理介质特性

传输媒体	数据速率	传输距离	性能（抗干扰性）	价　格	应　用
双绞线	10Mbps~1000Mbps	< 100m	可以	低	模拟/数字传输
50Ω同轴电缆	10Mbps	< 1km	较好	略高于双绞线	基带数字信号
75Ω同轴电缆	<300Mbps	100km	较好	较高	模拟传输电视、数据及音频
光纤	160Gbps	<110km	很好	较高	远距离传输
短波	<50Mbps	全球	较差	较低	远程低速通信
地面微波	<500Mbps	< 1000km	好	中等	远程通信
卫星	256Kbps	<18000km	很好	与距离无关	远程通信

一旦确定了上表中的物理介质类型，还需要根据实际需要，确定具体的产品类型，例如：

- 双绞线：分为屏蔽线和非屏蔽线，其中非屏蔽线主要应用的有 3 类线、5 类线、6 类线。
- 50Ω同轴电缆：分为粗缆和细缆。
- 光纤：分为单模与多模，产品则以纤径、光缆内纤数、外壳材质不同而区分。
- 卫星：根据通信频段和天线口径，分为 VSAT（Very Small Aperture Terminal，甚小口径卫星终端站）和 BGAN（Broadband Global Area Network，宽带全球网络）。

2．网卡

网卡是在介质确定后的物理层元素之一，因为网卡必须与网络的物理介质、拓扑结构和 MAC 层协议相匹配。在选择网卡或者决定现存的网卡是否满足需要时，可以参考表 2-15 的网卡特征表。

表 2-15　网卡特性表

支持的局域网	以太网、FDDI、快速以太网、千兆以太网、Arcnet、ISDN、令牌环网
支持的计算机总线	MCA、ISA、EISA、PCI、NubUS、VME、USB
RAM 缓冲大小	8Kbps、16Kbps 和 32Kbps
总线大小	8 比特、16 比特和 32 比特
数据速率	4Mbps、10Mbps、16Mbps、100Mbps、1Gbps
介质类型	10Base2、10BaseT、UTP、STP、光缆
支持的旧版本	VINES、NetWare、Apple Talk 和 Microsoft Windows NT 等
价格和功能	检查当前供应商的说明书

2.5.4 局域网技术选择与应用

2.5.4.1 生成树协议

在局域网络中，交换设备间借助于生成树协议（Spanning-Tree Protocol，STP）来完成动态“修剪”第二层交换机，而形成统一的树型结构，避免数据链路层环路的存在，其标准为IEEE802.1D。

对于采用交换机实现局域网段物理划分的网络来说，生成树协议是实现交换机设备间透明桥接的关键协议，设计人员将交换机的物理连接设计成有冗余和可扩展的结构，而协议运行的结果将禁用某些端口和连接，使得网络设备之间形成逻辑的树型结构。

交换机之间通过发送桥接协议数据单元（BPDU）来建立和维护生成树，协议在交换机启动时就参与了STP的收敛过程，当设备的端口、连接发生变化时，也会发送维护数据单元。

1．STP收敛过程

交换机遵循下面4个步骤将网络结构收敛到一棵树：

（1）从交换机中选择一个作为根网桥。

（2）在每台交换机上选择一个端口，被称为根端口，该端口提供到根网桥的最低开销路径。

（3）在每个局域网段互联的多个交换机中，选择一个作为指定网桥，并从该交换机上选取指定端口。

（4）决定哪台交换机的端口添加到生成树的结构中，所有被选择的端口都应该是根端口或者是指定端口。

每次交换机启动，都会假设自己是根网桥，通过BPDU将自己的桥ID与其他交换机的进行比较，确定最小者为真正的根网桥；在协议运行过程中，交换机能够收到BPDU的端口都将记录收到的最优BPDU，由最优BPDU来决定算法的运行，确定最优BPDU的顺序标准如下：

- 最小根网桥ID。
- 到根网桥的最低路径开销。
- 发送者最小桥ID。
- 最小端口ID。

基于这些BPDU，交换机的所有端口在启动后将经历以下4个阶段。

- 阻塞：只接收BPDU。
- 监听：创建生成树。
- 学习：创建交换（桥接）表。
- 传输：发送和接收用户数据。

2．选择根网桥

设计者在进行了带有冗余的局域网结构设计之后，如果任由 STP 进行修剪，由于根网桥的选择主要基于桥 ID，则很有可能导致中心的、可靠的、高速的交换机不能成为根网桥，而低速的交换机成为根网桥。网络设计者应该避免这种情况的发生。

根网桥是具有最小桥 ID 的交换机，桥 ID 有两个部分，优先权字段和交换机 MAC 地址，大多数厂商都带有自己的统一默认优先权，这样当这些交换机互连时，最小的 MAC 地址交换机就成了根网桥。

设计人员必须针对生成树协议，对交换机的优先权部分进行手工设置，通过确保特定的交换机拥有较小的优先权，来避免低速、非核心交换机成为根网桥。不同的设备厂商对优先权的配置方法不同，但是设计人员在这个阶段，只要确定局域网络中交换机的优先级别就行了。

3．根保护

有些网络设备可以提供根网桥的保护，可以防止低速交换机抢占根网桥。在交换机上配置根保护的端口不能作为根端口，而是作为局域网段的指定端口，如果在此端口上收到更优的 BPDU，根保护会禁用这一端口，而不是采用这一 BPDU 和选用新的根网桥。

根保护功能需要在所有不应该成为根网桥的交换机的所有端口上开启，避免这些端口可能成为根端口。

4．STP 更新时间

在生成树创建以后，STP 协议会根据连接关系的变化而产生更新过程。一般情况下，STP 协议更新的时间为 30s——2 倍的默认传送时延计时，而一些特殊的情况会导致更新时间长达 50s——最大计时与 2 倍的默认传送时延计时之和；其中默认传送时延计时为 15s，默认最大计时为 20s。

因此，一旦网络中出现较大的连接关系变化，则意味着局域网络可能中断 30s 或者 50s，这对于大多数网络应用来说，是可以接受的；但是对于有些特殊应用而言，则是不可忍受的；对于承载了这些应用的局域网络来说，只能修改 STP 的传送时延计时与最大计时的值（这会导致大量的 BPDU 和交换设备 CPU 资源的浪费），或者采用其他的链路保护技术。

2.5.4.2 扩展生成树协议

对于当前越来越复杂的网络，单纯使用基于 IEEE 802.1D 的生成树协议，已经不能满足网络用户在网络结构发生变化时的需求，所以需要在生成树协议基础上，形成相应的扩展。

1．快速生成树协议

快速生成树协议（Rapid Spanning-Tree Protocol，RSTP）的标准为 IEEE 802.1w，这是对 IEEE 802.D 的补充，通过对交换机端口的配置改变而实现 STP 的快速收敛。

RSTP 的核心思想是预先对生成树的拓扑结构以及可能发生的变化进行设定，一旦网络中连接关系发生变化，则整个网络的生成树会依据预先设定的拓扑收敛，这样减少了 STP 重新配置和恢复服务所需的时间，同时也保持了 STP 即插即用的特色。

RSTP 将优先级最高的交换机设定为根桥，并给各端口分配相应的端口角色，这些端口角色包括根、指定、替换与备份；在 STP 的拓扑收敛时，借助于端口角色完成快速收敛。

2. 基于 VLAN 的扩展协议

在传统 STP 协议中，每个 VLAN 都会单独维护自己的生成树，这样在网络中的一个连接发生变化时，多个 VLAN 的生成树都要发生变化；而基于 VLAN 的扩展协议充分利用多个 VLAN 中生成树的类似特性，减少链路变化和 VLAN 生成树运算对网络的整体影响。不同组织和网络设备公司都提供了 STP 的 VLAN 扩展协议。

IEEE 使用多生成树标准（MST）增强了原始的生成树算法，即 IEEE802.1s，该协议提高了 RSTP 的扩展性，将一组基于 VLAN 的生成树聚合成不同的实例，可以提供多条数据转发路径，实现负载均衡。

extreme 公司提出的 ESpan 技术，这是一种在环状网络中，实现多个 VLAN 的生成树维护和快速收敛技术。

Cisco 公司提出的“BPDU 倾斜检测”功能，允许交换机跟踪和检测各种 BPDU，并以系统日志的方式通知管理员。同时提出了多实例生成树协议(MISTP)，允许一组 VLAN 来共同使用一棵生成树。

2.5.4.3 虚拟局域网

虚拟局域网（VLAN）基本上可以看作是一个广播域，是根据逻辑位置而非物理位置划分的一组客户工作站的集合，这些工作站不在同一个物理网络中，但可以像在一个普通局域网上那样进行通信和信息交换。VLAN 是局域网建设中的重要内容，围绕 VLAN 的主要设计内容包括：

- VLAN 划分方法。
- VLAN 划分方案。
- VLAN 的跨设备互连。
- VLAN 间路由。

1. VLAN 划分方法

VLAN 划分方法是指采用何种标准，以确定 VLAN 中节点的方法。

VLAN 划分方法主要包括下述 5 种：

- 基于设备端口。
- 基于 MAC 地址。
- 基于网络地址。

- 基于 IP 组播。
- 基于策略。

不同的划分方法适用于不同的网络应用需求。

1）基于设备端口

最常用的 VLAN 划分方法就是基于设备端口，通过将设备上的端口划归不同 ID 的 VLAN，使得设备端口连接的计算机节点隶属于不同的 VLAN；由于设备的端口与计算机节点的物理位置有关联，因此该种方法其实是基于计算机节点的物理位置来进行 VLAN 划分的。

这种方法配置比较简单并且有效，但它不允许多个 VLAN 同时包括同一物理网段，其最主要的限制是：当某个用户从一个端口改到另一端口时，网络管理员将不得不对 VLAN 成员进行重新配置。

大多数局域网络的 VLAN 划分都采用基于设备端口的方式，在设计阶段，设计者需要确定局域网络内存在多少 VLAN，并给不同 VLAN 分配 ID 号，同时需要通过端口表来确定各端口应加入的 VLAN 号。

2）基于 MAC 地址

基于 MAC 地址是指网络管理人员必须确定每个 VLAN 中各计算机节点的 MAC 地址，也就是为每个 VLAN 形成一个 MAC 地址库，只有属于同一个 MAC 地址库的计算机节点才允许通信。

由于 MAC 地址是网卡的唯一标识，计算机在局域网络内部发生物理位置变化时，不会导致 VLAN 的变化，因此基于 MAC 地址的划分方法是屏蔽了计算机节点物理位置的。

这种方法适用于网络节点流动性较大，但是计算机之间分组关系相对稳定的局域网络，存在以下优缺点：

- VLAN 不会因为计算机节点的流动而产生变化和重新配置。
- 同一个 MAC 地址可以处于多个 VLAN 中。
- VLAN 的 MAC 地址库初始化工作量较大。
- 一旦用户计算机更换网卡，就必须进行 VLAN 数据库的更新，否则用户无法访问网络。
- 对于临时出现在局域网中的便携计算机，则必须由管理员加入 VLAN 数据库才能访问网络。

3）基于网络地址

基于网络地址的划分方法，主要是借助于第 3 层协议的地址来确定 VLAN 成员，常用的网络层地址是 IP 地址。在设计基于网络地址的 VLAN 划分方式时，需要确定 VLAN 和网络地址段之间的关系，例如对于不同 ID 的 VLAN，确定其使用的 IP 地址段。

采用基于网络地址的划分方法适用于网络安全性要求不高，用户组经常发生变动的

网络，其存在的优缺点如下：

- 用户的网卡调换，只要不重新分配地址，不会对 VLAN 产生影响。
- 用户在进行 VLAN 间切换时，只需要修改相应的网络地址，如 IP 地址。
- 利用实现基于服务或基于应用的各种策略。
- 对于网络设备来说，减少了数据帧标记的消耗。
- 缺乏安全性。
- 对网络地址的处理会带来较大的资源损耗。
- 网络管理员对用户的控制能力降低。

4）基于 IP 组播

IP 组播代表着一种与众不同的 VLAN 划分方法，各站点可以自由地动态决定参加到哪一个或哪一些 IP 组播组中。一个 IP 组播组实际上用一个 D 类地址表示，当向一个组播组发送一个 IP 报文时，此报文将被传送到此组中的各个工作站点处，这实际上就是一个特定的 VLAN。

基于 IP 组播的 VLAN 就是针对不同的 IP 组播地址建立不同的 VLAN，这种 VLAN 中的各个成员都是临时节点，节点可以随时宣布加入和退出组播组；该种方法适用于网络中存在大量基于组播应用的情况。

5）基于策略

基于策略的划分方法，是实施 VLAN 划分最复杂的方法，其划分能力也最强；建立 VLAN 的标准不再是一种规则，而是多种规则的综合；也就是说该方法允许网络管理员使用任何 VLAN 策略的组合来创建满足其需求的 VLAN。

在实施策略制定时，不仅仅局限于上面提到的任何一种 VLAN 划分策略，还可以根据应用协议来添加策略；因此基于策略的 VLAN 划分方法具有较强的灵活性，但是一旦发生变化，其调整的难度也相应加大；另外这种划分方法对网络管理人员的要求较高。

2．VLAN 划分方案

VLAN 划分方案主要指的是在进行 VLAN 划分时，应如何划分多个 VLAN，由于基于端口划分的方法最常用，而其他划分方法具有较多不确定性，因此本文仅给出基于端口划分方案中应考虑的内容。

1）管理 VLAN

管理 VLAN 是由网络管理人员专用的网络，一般情况下，管理 VLAN 中节点主要包括以下内容：

- 大型网络设备一般提供网络管理方式，因此所有网络设备的管理端口都应加入管理 VLAN。
- 大型服务器也会提供特殊的远程管理网络端口，这些端口不对外提供服务，只提供远程访问服务，也应该加入管理 VLAN。
- 各种设备向网管服务器提交 SNMP 协议数据的网络端口。

- 网管平台服务器和网管工作站。

通过划分管理 VLAN，并对管理 VLAN 划分特殊 VLAN ID 号和网络层地址，可以增强网络管理工作的安全性，避免用户对网络管理设备的直接访问，是非常有必要的。

管理 VLAN 可以与其他 VLAN 不进行连通，以确保网络管理的安全性。

2）服务器 VLAN

服务器是向局域网络提供服务的关键，大多数情况下，局域网内部的服务器都位于局域网的核心部分，针对服务器群建立一个特定的 VLAN，可以加强服务器之间的访问，同时提高了服务器的运行安全性。

对于网络中服务器较多的情况，还不能仅仅划分为一个 VLAN，可以根据服务器的服务内容进行更细的 VLAN 划分，例如管理类服务器 VLAN、应用服务器 VLAN、数据库服务器 VLAN 等。

针对服务器划分 VLAN 的优势在于可以针对这些 VLAN 的网络地址设定特定的访问控制策略，以增强服务器的运行安全性。

3）用户的部门 VLAN

在网络使用中，相同的部门用户，其所需要的应用服务基本是一致的，因此可以针对用户计算机的部门分布情况，划分不同的 VLAN，例如财务 VLAN、生产 VLAN、销售 VLAN 等。

可以针对不同部门的 VLAN，制定不同的访问控制策略，以提高整个网络的安全性。

3. VLAN 的跨设备互连

在基于设备端口的 VLAN 划分方式中，一台交换机上可能存在多个 VLAN 的端口，但同时，一个 VLAN 的端口，也可以分布在不同的交换机设备上。为了实现不同交换机上相同 VLAN 端口间的互访，必须借助于 VLAN 的跨设备互连协议。

一般来说，在基于端口方式下，网络端口可以处于以下几种状态：

- 静态访问端口（static-access）：该类端口只能属于一个 VLAN，并且一旦设定，将不再发生变化，除非修改端口所属的 VLAN ID。
- 动态访问端口（dynamic-access）：该类端口可以动态地加入 VLAN，并且可以加入多个 VLAN，这种方式在具体应用中很少出现。
- VLAN 互连端口（trunk）：该类端口主要用于不同交换机间的 VLAN 数据帧传递，该端口主要通过对数据包进行封装，并加入 VLAN 标记信息的方式，将数据帧传递给其他设备，由其他设备进行解析后，传递至相应的 VLAN。

对于静态访问端口，其配置方法较为简单，仅仅需要配置该端口属于相应的 VLAN 就行了；但是对于 VLAN 互连端口，则需要考虑的配置就相对复杂得多；对于 Trunk 端口，一般需要考虑以下配置信息：

- Trunk 端口允许互连的 VLAN。如果某一个 VLAN 不在当前 Trunk 端口的允许互连 VLAN 范围中，就意味着本交换机不能利用这个端口将封装好的该 VLAN 帧

传递给其他交换机；对于这个 VLAN 来说，该 Trunk 端口就是相当于生成树中的一个被阻塞端口。网络设计中，允许不同的 VLAN 借助于不同的 Trunk 端口来实现设备互连，例如所有单号 VLAN 利用 Trunk 端口 1 互连，而所有双号 VLAN 利用 Trunk 端口 2 互连。

- 封装协议。各种网络设备的厂商，都可以设计其独有的 VLAN 封装协议，例如 Cisco 公司提供的 ISL 协议；对于不同厂商的设备互连来说，只能选择标准的 IEEE 802.1Q 协议，否则无法互连；对于相同厂商的设备来说，只要互连的两个 Trunk 端口使用相同的封装协议就可以完成 VLAN 的跨设备互连。
- Trunk 端口的默认 VLAN。Trunk 端口也是属于一个 VLAN 的，这个 VLAN 被称为该端口的默认 VLAN；需要注意的是，在数据帧传递过程中，Trunk 端口对不是默认 VLAN 的数据帧都是封装后才传递，而对于默认 VLAN 的数据帧，则不进行封装；因此，两个互连的 Trunk 端口，除了允许通过的 VLAN 要相同之外，其默认 VLAN 也必须一致；假如网络中存在 10 个 VLAN，交换机 1 的 Trunk 口的默认 VLAN 为 1，交换机 2 的 Trunk 口的默认 VLAN 为 2，两个 Trunk 口允许所有的 VLAN 通过，则会产生除了 VLAN 1 和 VLAN 2 不通，其他 VLAN 都是互通的奇特情况。

4．VLAN 间路由

VLAN 间是无法在数据链路层连通的，只能借助于网络层协议连通。

实现 VLAN 间路由需要借助于网络层设备——路由器，图 2-49 所示是利用路由器实现 VLAN 间路由的两种方式。

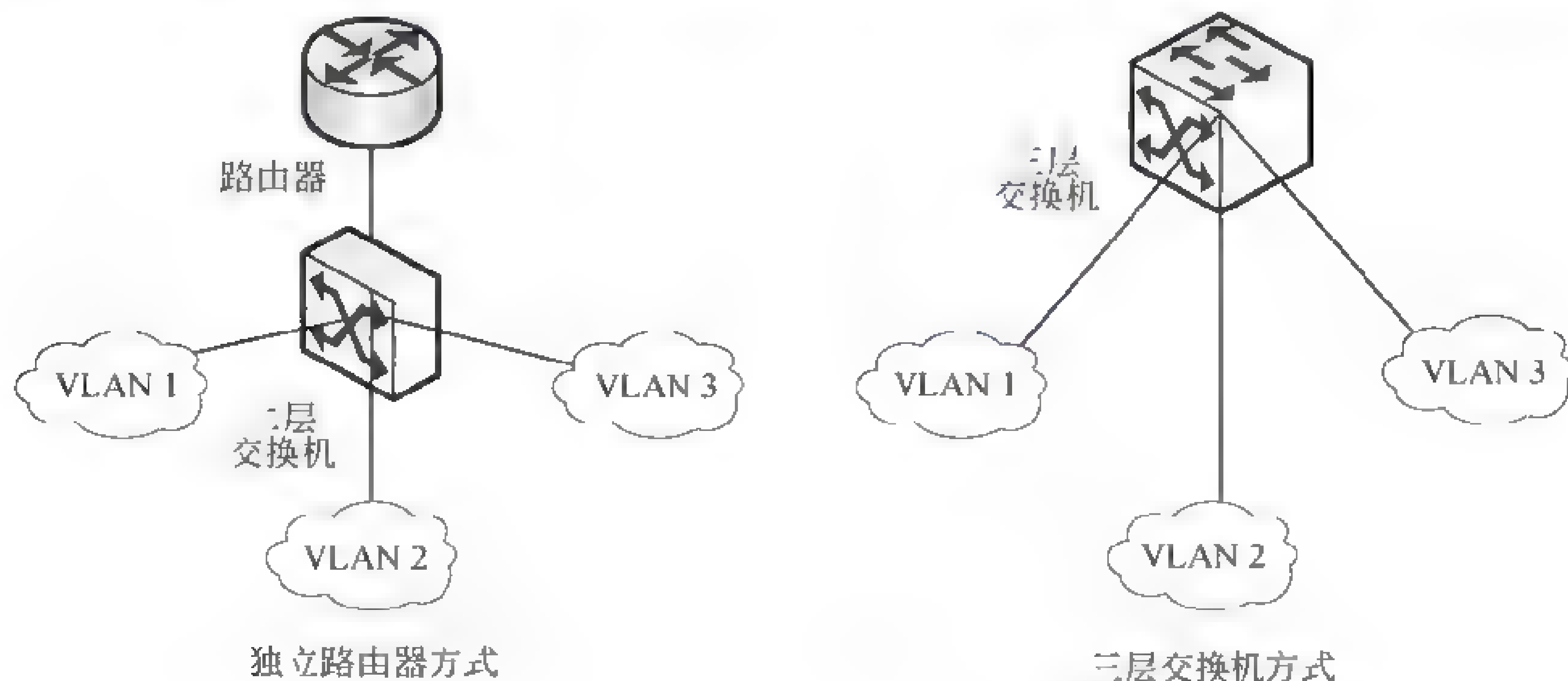


图 2-49　实现 VLAN 间路由的两种方式

1）借助于独立路由器

对于只能提供数据链路层功能的交换机来说，划分的 VLAN 是无法直接连接的，必

须借助于独立的路由设备。在使用独立的路由器时，路由器只需要一个端口接入到二层交换机；在这个物理端口上，将定义若干个逻辑端口，每个端口都接入不同的 VLAN，则 VLAN 间就借助于路由器实现了互连，这种方式被形象地称为独臂路由器方式；在通信过程中，VLAN 间数据帧要被解封成 IP，才能经过路由器进行传递。

2）借助于三层交换机

如果网络中存在着三层交换设备，由于三层交换机具有路由功能，可以直接实现多个 VLAN 之间的通信。三层交换机就相当于一个中心路由器，每个 VLAN 都是该路由器的直接连接网络，这些 VLAN 之间只需要进行简单的路由交换，而不需要复杂的路由计算，就可以完成连通。

三层交换机与独立路由器不同的是，三层交换机不需要对所有的 VLAN 数据包进行解封、重新封装操作，可以基于“一次路由、多次交换”原理的 VLAN 间线速交换替代数据包的路由。

目前借助于三层交换机实现 VLAN 间通信是局域网设计的主流方法。

2.5.4.4　无线局域网

在园区网络中，无线局域网络可以满足移动用户对内部网络和因特网的接入需求。一个无线局域网络是由 AP 组成，该设备利用射频和无线用户通信，一个 AP 能够覆盖的区域称为无线单元。

设计一个无线局域网结构需要设计者了解一个无线单元的覆盖区域大小、需要多少个无线单元才能满足整体区域的覆盖需求，其中影响无线单元的因素包括数据速率、电源、天线功率和位置，同时安装现场的建筑特性也会影响覆盖区域。

设计无线局域网络需要考虑以下三个部分的内容。

1．定位 AP 实现最大覆盖率

理论上的 AP 信号覆盖区域是一个三维的球体，而 AP 处于中心的位置上；由于大多数 AP 多是全方位天线，通常是 4～6 英寸的发射器件，连接在一个可旋转或可定位的轴上；天线的信号强度在垂直于天线轴的方向最强，而平行于天线轴的方向最弱，其覆盖的区域就像一个轮胎的内胆。

AP 可以安装在一个水平或垂直的位置上，但是要确保全方位天线指向正上方；对于数据传输速率，可以通过改变电源或使用的天线来改变覆盖区域或覆盖的形状；同时，墙壁等障碍物可以衰减信号的强度，但不会完全阻挡信号。

在设计工作中，应对无线网络 AP 设备的信号覆盖进行预测，明确满足数据通信的信号覆盖区域，再依据区域范围设计各 AP 的位置，同时对多个 AP 信号覆盖的交界位置应重点进行测试，保证整个区域的整体覆盖。

2．无线局域网中的虚拟局域网设计

在整体无线局域网覆盖区域中存在多个 AP 设备，用户在覆盖区域内移动时，由于

信号的强弱，会选择不同的 AP 设备进行通信。AP 设备需要通过网络线路连接至有线网络，并可以对接入的无线网卡自动分配或者手动分配 IP 地址。

在对无线局域网络的虚拟网络设计中，为了保证用户可以自由漫游同时保持对网络资源的不断访问，可以将所有的 AP 的地址都放在一个 IP 子网内，也就是说在一个虚拟局域网络中；这样连接的无线网卡之间通信较为简单，同时其切换 AP 时丢失正在传输数据包的可能性降到了最低。

当然，如果无线网络用户过多，可以根据应用或者地理位置划分为多个虚拟局域网，但是网卡从一个网段的 AP 切换到其他 AP 时，必然会导致数据包的丢失。

3．冗余无线接入点

无线局域网络同样可以实现冗余，部分厂商提供了 AP 的热备份功能，这种技术容许在一个覆盖区域中使用两个 AP，并共享同一个频道；其中一个主 AP 是活跃的，而备份 AP 监控主 AP 和网络运行的情况，一旦主 AP 出现故障，则由备份 AP 进行替代；主用和备用 AP 间的距离较小，除了 IP 地址不同，其他配置基本一致；另外，主 AP 恢复后需要用户进行手工操作来完成备用至主用的切换。

4．网络 SSID

无线 AP 的 SSID 是无线单元的名称，在一个园区网络的无线局域网络中，所有的无线 AP 都应该配置成一样的 SSID。

2.5.4.5 线路冗余和负载分担

局域网交换机之间设计冗余链路是较为常见的做法，对于这些冗余链路则存在着备份和负载分担两种应用方式。

1．备份方式

对于大多数局域网络来说，虽然网络中交换机之间存在着链路的冗余，但是由于 IEEE 802.1D 标准中 STP 算法的运行，导致这些网络设备之间的冗余链路只能有一条生效，而其他链路处于备份状态，一旦主用链路失效，经过 STP 计算收敛，将使得备份链路生效。

在这种方式下，网络必然存在交换机或者链路处于闲置的状态，导致资源的浪费。

2．负载分担方式

由于局域网络中存在多个 VLAN，实际上每个 VLAN 都必须维护自己的生成树，因此可以通过将冗余设备和冗余线路分配到不同的 VLAN 中并分配不同的角色，实现负载的分担。例如，某台交换机对于一些 VLAN 来说是根网桥，而对于另外一些 VLAN 来说则是备份根网桥。

通过这种方式，可以避免冗余设备和冗余链路在网络中的闲置，实现负载分担。

在所有的基于 VLAN 的生成树扩展协议中，都可以实现负载分担方式，仅仅是配置的方法和命令存在着差异。

2.5.4.6　交换机设备应用

交换机作为局域网的核心设备，除了常规的数据帧的存储与转发功能之外，还有一些特殊的应用，这些应用可以满足局域网络用户的一些特殊需求，主要包括链路聚合、冗余网关、以太网供电、多业务模块等。

1．链路聚合

链路聚合是将两个或更多数据信道结合成一个单个的信道，该信道以一个单个的更高带宽的逻辑链路出现。链路聚合一般用来连接一个或多个带宽需求大的设备，例如连接骨干网络的服务器或服务器群。

如果聚合的每个链路都遵循不同的物理路径，则聚合链路也提供冗余和容错。通过聚合调制解调器链路或者数字线路，链路聚合可用于改善对公共网络的访问。链路聚合也可用于企业网络，以便在吉比特以太网交换机之间构建多吉比特的主干链路。

如图 2-50 所示，采用链路聚合后，逻辑链路的带宽增加了大约（n−1）倍，n 为聚合的路数。另外，聚合后，可靠性大大提高，因为 n 条链路中只要有一条可以正常工作，则这个链路就可以工作。除此之外，链路聚合可以实现负载均衡，通过链路聚合连接在一起的两个（或多个）交换机（或其他网络设备），通过内部控制，也可以合理地将数据分配在被聚合连接的设备上，实现负载分担。

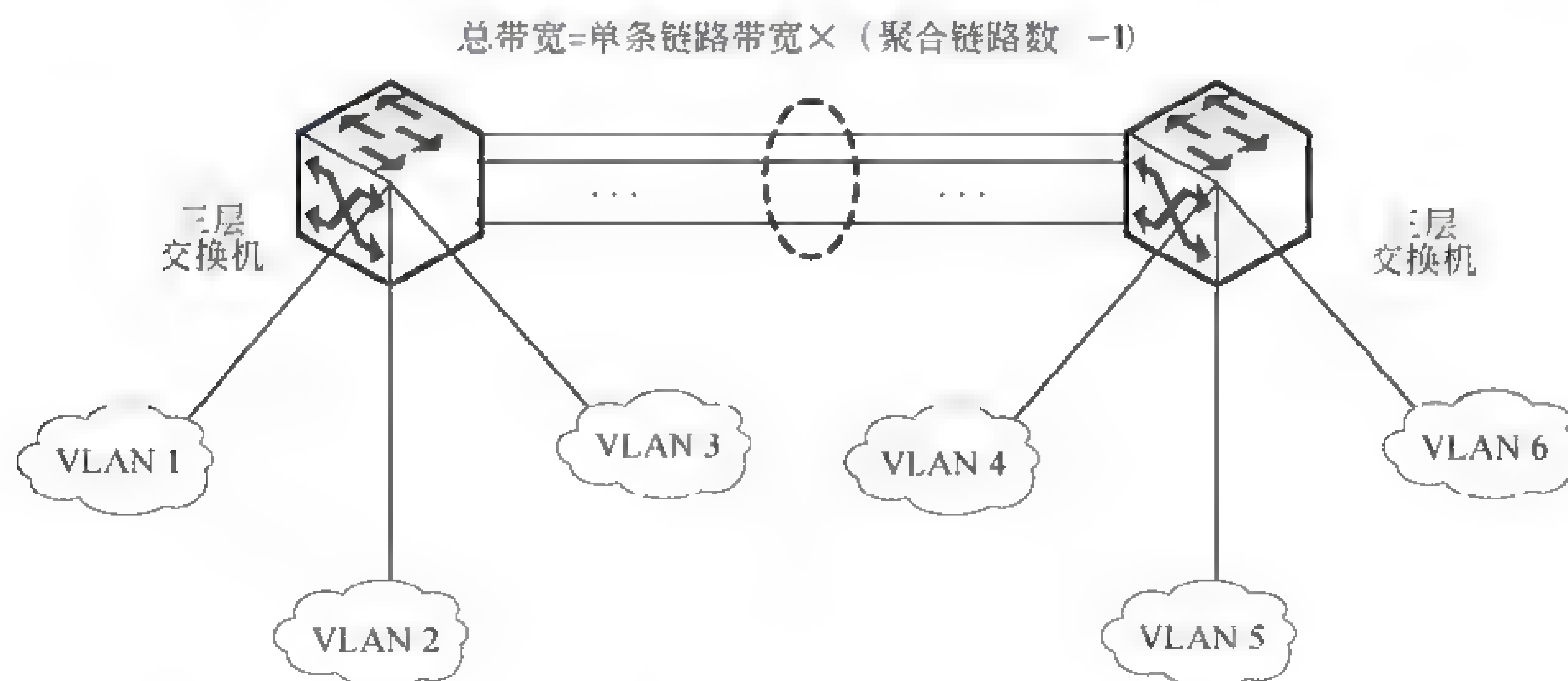


图 2-50　链路聚合示意图

2．冗余网关

对于由多个 VLAN 构成的局域网络来说，每个 VLAN 的网关设备多是由核心交换机来承担，一旦核心交换机出现故障，则多个 VLAN 的网关都将出现问题，这些 VLAN 之间的通信将处于中断状态。为了避免这种情况的发生，大多数核心交换机都会提供冗余网关协议，使得网络中至少两台交换机成为各个 VLAN 的网关，避免网关的单点故障

效应。

常见的冗余网关协议包括通用的虚拟路由器冗余协议（Virtual Router Redundancy Protocol，VRRP）和由 Cisco 公司提供的热备份路由器协议（Hot Standby Router Protocol，HSRP）与网关负载均衡协议（Gateway Load Balancing Protocol，GLBP）。

1）VRRP

虚拟路由器冗余协议（VRRP）是一种选择协议，它可以把一个虚拟路由器的责任动态分配到局域网上的 VRRP 路由器组中的一台。控制虚拟路由器 IP 地址的 VRRP 路由器称为主路由器，它负责转发数据包到这些虚拟 IP 地址。一旦主路由器不可用，这种选择过程就提供了动态的故障转移机制，这就允许虚拟路由器的 IP 地址可以作为终端主机的默认第一跳路由器。使用 VRRP 的好处是有更高的默认路径的可用性而无须在每个终端主机上配置动态路由或路由发现协议。

图 2-51 为 VRRP 协议的应用方式，VRRP 将局域网的一组路由器（包括一个 Master 即活动路由器和若干个 Backup 即备份路由器）组织成一个虚拟路由器，称为一个备份组。这个虚拟的路由器拥有自己的 IP 地址 202.114.64.1，备份组内的路由器也有自己的 IP 地址（如 Master 的 IP 地址为 202.114.64.2，Backup 的 IP 地址为 202.114.64.3）。局域网内的主机仅仅知道这个虚拟路由器的 IP 地址 202.114.64.1，而并不知道具体的 Master 路由器的 IP 地址 202.114.64.2 以及 Backup 路由器的 IP 地址 202.114.64.3。如果备份组内的 Master 路由器坏掉，Backup 路由器将会通过选择策略选出一个新的 Master 路由器，继续向网络内的主机提供路由服务。从而实现网络内的主机不间断地与外部网络进行通信。

VRRP 协议最大的缺点在于只有主用路由设备处于活跃状态，而其他路由器都处于热备状态，导致备用路由器闲置。为弥补这个缺陷，在实际应用中，可以对于不同的 VLAN 指定不同的主用和备用路由器，从而让所有路由器都发挥作用。

2）HSRP

热备份路由协议（HSRP）是 Cisco 公司独有的技术，为 IP 网络提供了容错和增强的路由选择功能，通过使用同一个虚拟 IP 地址和虚拟 MAC 地址，LAN 网段上的两台或者多台路由器可以作为一台“虚拟”路由器而对外提供服务。LAN 网段上的主机都配置使用同一个虚拟路由器作为默认网关，并不断将 IP 包发往同一个 IP 和 MAC 地址。

HSRP 中的路由器组中存在多种角色，一个 HSRP 路由器组中最少需要两台路由器。

- 活跃路由器：转发发送到虚拟路由器的数据包，通过发送 Hello 消息来承担和保持活跃的角色。
- 备份路由器：监视 HSRP 组的运行状态，当活跃路由器不运行时，承担转发数据包的责任；传输 Hello 消息，告知组中所有路由器备份路由器的角色和状态。
- 虚拟路由器：最终代表一台可以连续工作的路由器，由虚拟的 IP 地址和 MAC 地

址组成，但并不实际转发数据包。

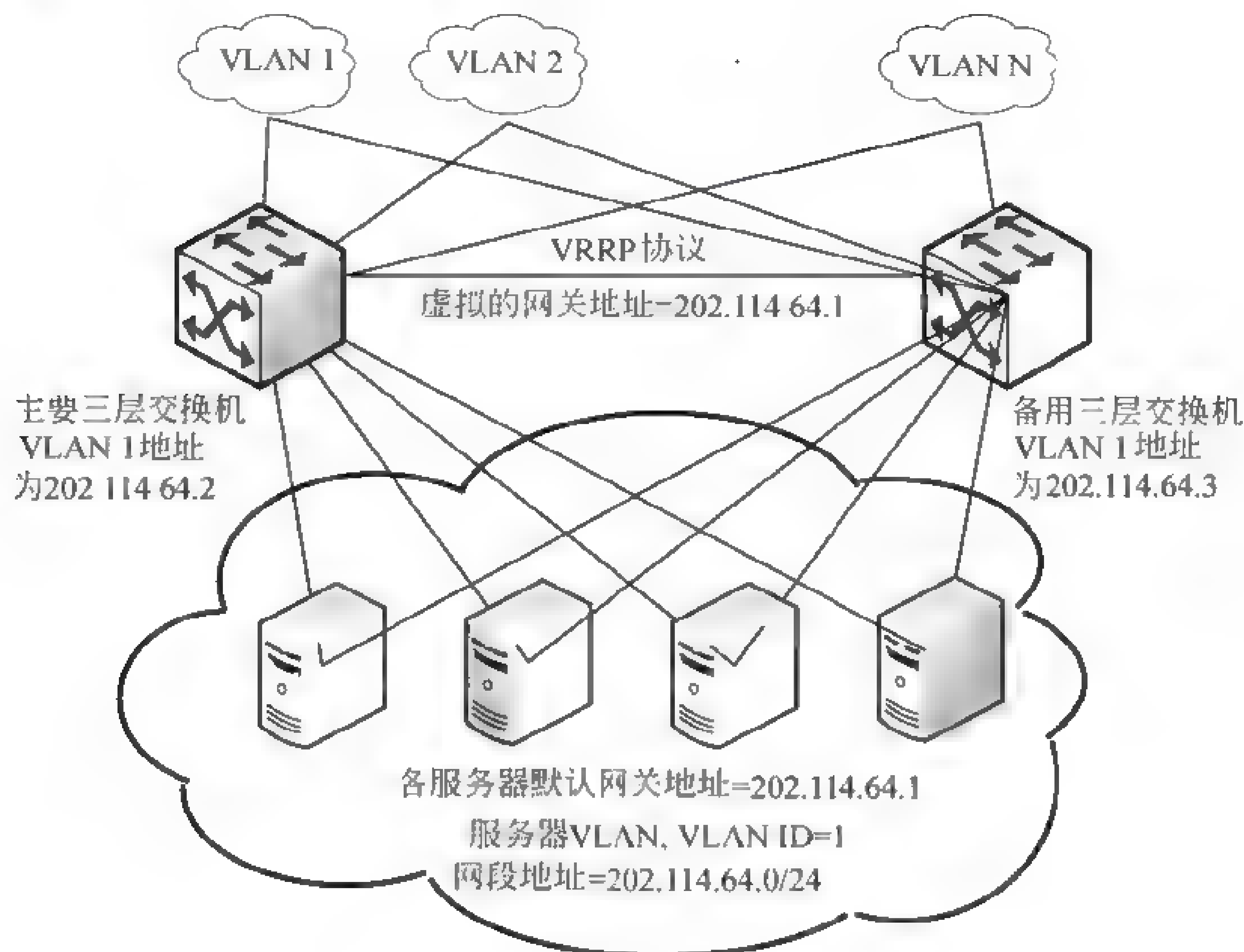


图 2-51　VRRP 应用示意图

- HSRP 组路由器：监视 Hello 消息，但不应答；转发经由它们的数据包，但不转发经虚拟路由器的数据包。

HSRP 的使用方法和 VRRP 类似，同时也存在着路由器闲置的问题，不能实现负载分担，但是可以通过形成多个不同的虚拟路由器的方式，实现负载分担。

3）GLBP

GLBP 协议是 Cisco 公司提出的一种冗余网关协议，与 VRRP 和 HSRP 类似，但是可以实现负载均衡。

GLBP 实现负载均衡的方式是通过在多个路由器使用一个虚拟的 IP 地址和多个虚拟的 MAC 地址来实现负载均衡，主机的默认网关配置相同的 IP 地址，在虚拟路由器组里所有的路由器参与数据转发。

GLBP 组的成员会选举出一台路由器作为活动的虚拟网关（AVG），组中的其他成员在 AVG 有效的情况下提供对 AVG 的备份；AVG 对 GLBP 组中的每一个成员分配一个不同的虚拟 MAC 地址，并且通过对虚拟 IP 地址的 ARP 响应将不同的 MAC 地址通知给不同的访问计算机。每一个网关都根据其分配的 MAC 地址承担数据转发任务，因此被称为活动虚拟转发器（AVF）。

虽然 GLBP 技术出现较晚，但是由于其负载均衡的特性，已经开始逐步取代 VRRP、

HSRP 技术。

3. 以太网供电

以太网供电（Powder over Ethernet，POE）技术是通过以太网线路为 IP 电话、WLAN 接入点、网络摄像机等小型网络设备直接提供电源的技术。该技术可以避免大量的独立铺设电力线，以简化系统布线，降低网络基础设施的建设成本。

POE 技术是通过 4 对双绞线中空闲的 2 对来传输电力的，可以输出 44～57V 的直流电压、350～400mA 的直流电流，为一般功耗在 15.4W 以下的设备提供以太网供电；该技术可以在现有的以太网 5 类布线基础架构不作任何改动的情况下，为一些基于 IP 的终端（如 IP 电话机、无线局域网接入点 AP、网络摄像机等）传输数据信号的同时，还能为此类设备提供直流供电。

POE 技术能在确保现有结构化布线安全的同时保证现有网络的正常运作，最大限度地降低成本。一个典型的以太网供电系统如图 2-52 所示。在配线柜里保留以太网交换机设备，用一个带电源供电的集线器（Midspan HUB）给局域网的双绞线提供电源（也可以是大型交换机中的一个 POE 模块）；在双绞线的末端，该电源用来驱动电话、无线接入点、相机和其他设备；为避免断电，可以选用一个 UPS。

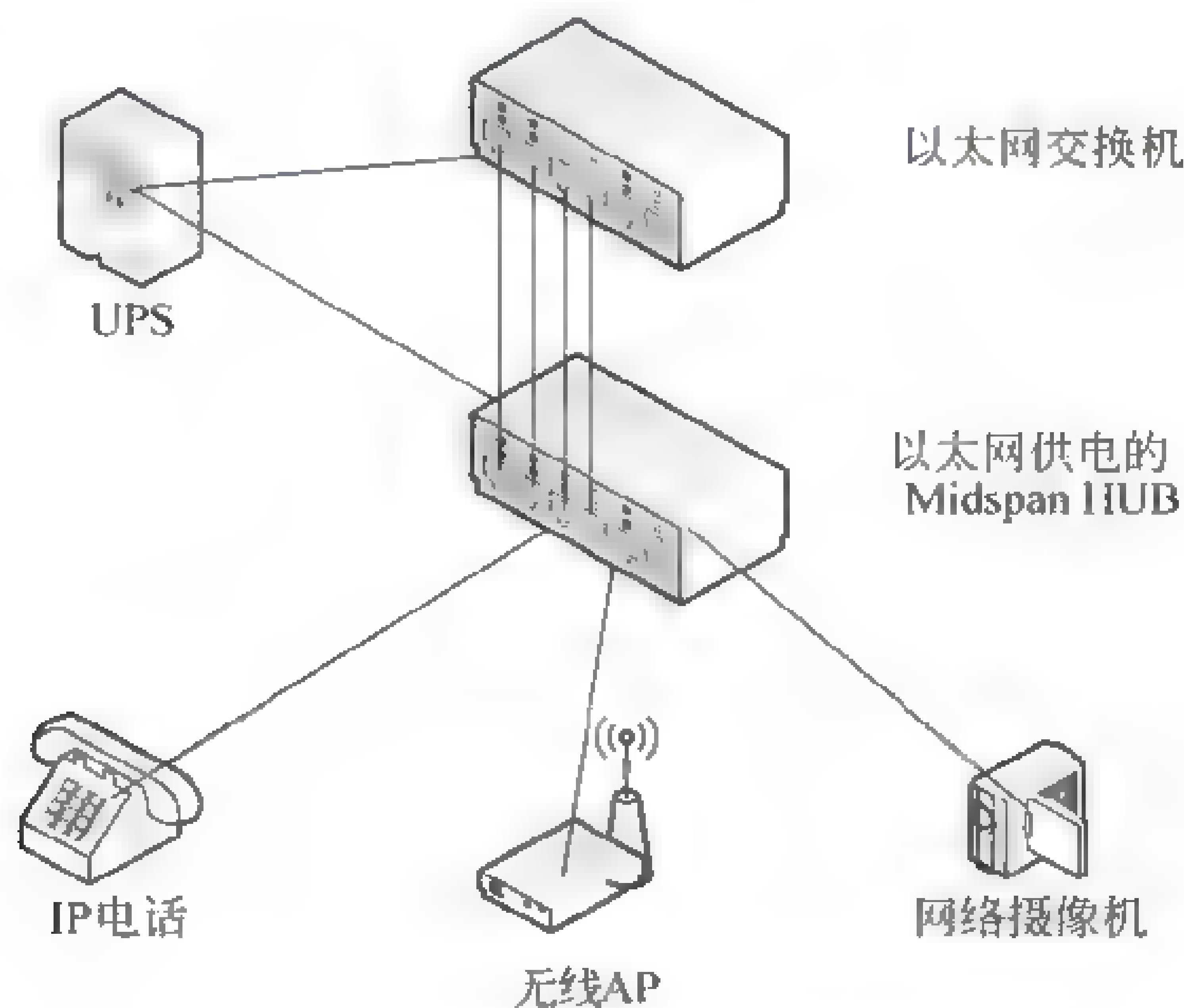


图 2-52 典型的以太网供电系统

4. 多业务模块

多业务模块功能，是指交换机生产厂商提供统一的业务模块接口，并提供特殊的业务功能开发包，由各业务功能设备提供商将产品封装成统一的交换机业务模块，使得业务服务可以直接从交换机框架上获取供电、网络数据，经业务处理后再发送至交换机框架上。

目前，常见的网络业务模块包括防火墙（firewall）、入侵者检测（IDS）、入侵者防御（IPS）、流量控制（FC）等，这些业务模块相对于独立的业务产品将提供更强的业务处理能力。

2.5.4.7　服务器冗余和负载均衡

为了提高服务器的性能和工作负载能力，企业通常会使用 DNS 服务器、网络地址转换等技术来实现多服务器负载均衡，特别是对外服务的 Web 网站，许多都是通过几台服务器来完成服务器访问的负载均衡。一般来说，实现服务器的冗余和负载均衡有多种方式。

1．使用负载服务均衡器

负载服务均衡器实际上是应用系统的一种控制服务器，所有用户的请求都首先到此服务器，然后由此服务器根据各个实际处理服务器状态将请求具体分配到某个实际处理服务器中，对外公开的域名与 IP 地址都是负载服务均衡器的域名或 IP 地址。

负载服务均衡器上需要安装负载均衡控制与管理软件，这台服务器一般只做负载均衡任务分配，但不是实际对网络请求进行处理的服务器。

负载服务均衡器为了将负载均匀地分配给内部的多个服务器，就需要应用一定的负载均衡策略，例如基于 CPU 繁忙程度或内存占用程度等。对于常见的 Web 服务，可以借助于负载服务均衡器让多台服务器设备提供服务；每台服务器的状态可以设为 regular（正常工作）或 backup（备份状态），或者同时设定为 regular 状态；负载服务均衡器根据设定好的负载均衡策略来将用户请求重定向到不同的服务器。

通过负载服务均衡器不仅可以实现各服务器群的流量动态负载均衡，并互为冗余备份，同时还具有一定的扩展性，可不断添加新的服务器到负载均衡系统。

2．使用网络地址转换

支持负载均衡的地址转换网关可以将一个外部 IP 地址映射为多个内部 IP 地址，对每次 TCP 连接请求动态使用其中一个内部地址，以达到负载均衡的目的。地址转换网关存在软件实现和硬件实现两种方式。

硬件实现方式指硬件厂商将这种技术集成在交换机中，作为第四层交换的一种功能；一般采用随机选择、根据服务器的连接数量或者响应时间进行选择的负载均衡策略来分配负载；但硬件实现方式的灵活性不强，不能支持更优化的负载均衡策略和更复杂的应用协议。

软件实现方式指在服务器上安装负载均衡的地址转换网关，可以对各服务器的 CPU、磁盘 I/O 或网络 I/O 等多种资源进行实时监控，并根据各种策略来转发客户对服务器的请求，因此具有较大的灵活性。

3．使用 DNS 服务器

使用 DNS 服务器来提供负载均衡是一种较为简单的方法，提供服务的多个服务器

独立运行，并拥有独立的 IP 地址，形成了一个可以提供服务的 IP 地址组；网络管理员在 DNS 服务器上进行注册，使得所有这些服务器的 IP 地址都拥有一个相同的域名，并对外只公布这个域名；当客户提交服务请求前，需要进行域名解析，DNS 服务器会针对这个域名的解析循环用 IP 地址组中的 IP 地址来应答，使得每次客户访问的服务器 IP 地址都不同，从而达到负载均衡。

使用 DNS 是一种简单的负载均衡方式，不可能根据各服务器的负载情况而动态调整 DNS 的解析，甚至服务器组中的一台服务器出现故障而不能提供服务时，DNS 仍不会将该服务器的 IP 地址从循环解析列表中清除，导致一部分请求失效。

4．高可用性技术

双机热备份高可用（High Availability，HA）系统，又称为高可用性集群，一般由两台服务器构成，通过对关键部件的冗余设计，可以保证系统硬件具有很高的可用性，对于一般非关键应用场合，其硬件系统的可用性可以达到 99.99%。在正常工作时，两台服务器同时工作或一台工作另一台热备，通过以太网和 RS232 口互相进行监测，并不断完成同步操作，数据保存在共享磁盘阵列中。

传统的高可用性集群的工作模式主要是单活（active/passive）、双活（active/active）。

1）单活

单活指服务器集群中，一台服务器处于活跃状态，对外提供服务；另外一台为热备方式，通过网卡和串行线路监控活跃服务器并实现数据同步；一旦发现活跃服务器出现故障，则通过 IP 地址漂移等技术接管服务，如图 2-53 所示。

2）双活

双活指服务器集群中，两台服务器都处于活跃状态，并同时提供服务，相互之间通过卡和串行线路监控并实现数据同步，一旦一台服务器出现故障，则另外一台服务器接管所有的服务负载，如图 2-54 所示。

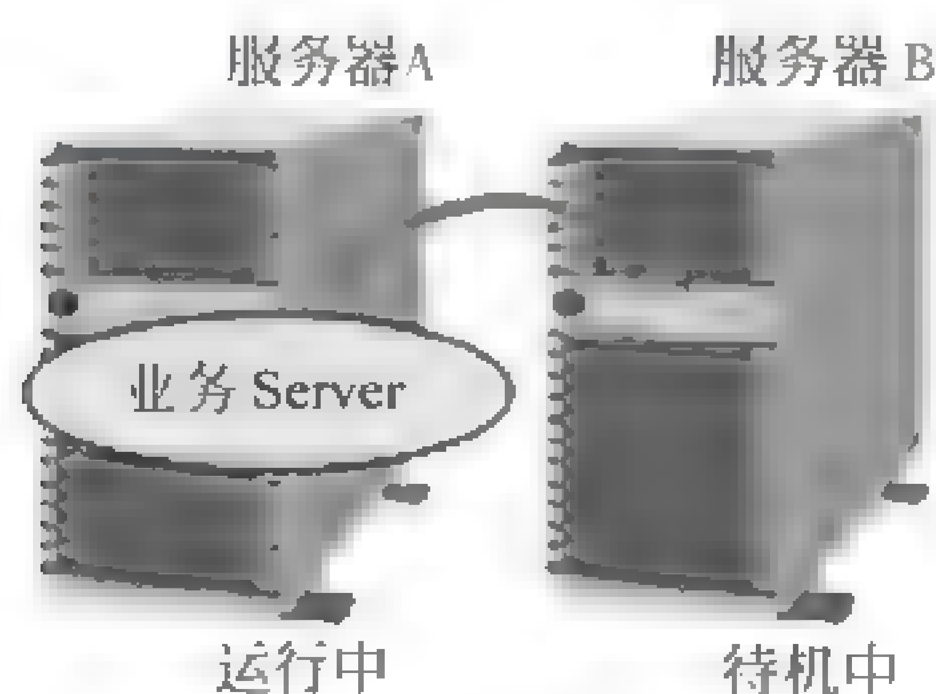


图 2-53　单活模式

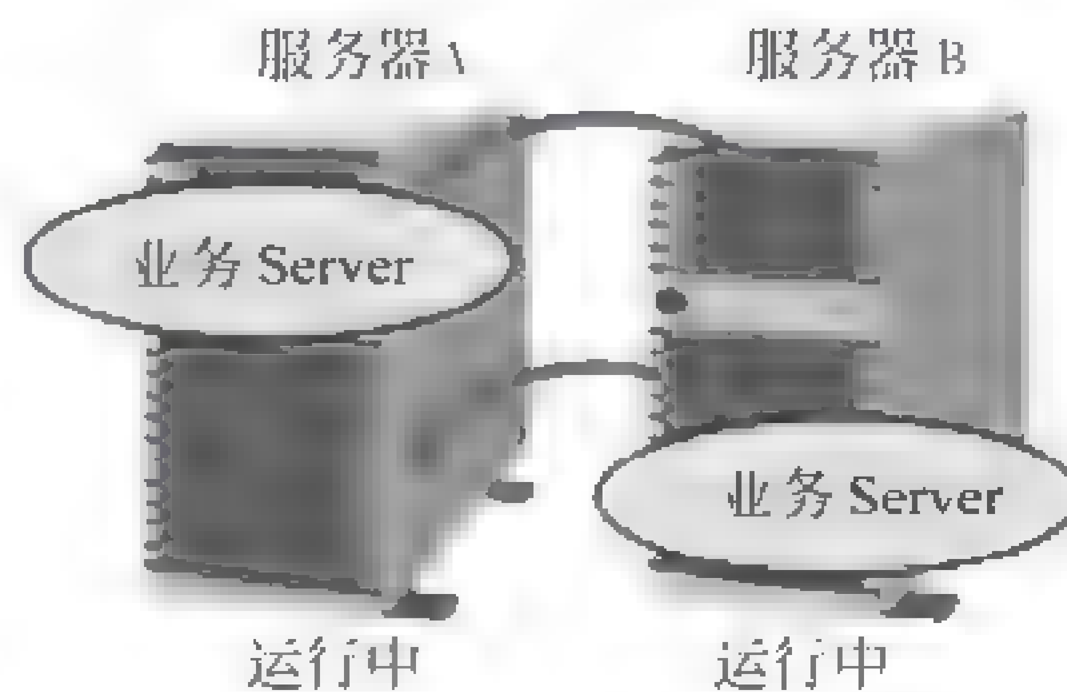


图 2-54　双活模式

高可用性服务集群主要应用于数据库服务器和各种应用服务器，这些服务器之间通过串行线路或者网络线路的心跳线来实现服务器监控和数据同步，并且所有服务器都通

过光纤通道连接至磁盘阵列，实现高速的磁盘访问。

服务器操作系统一级的高可用性集群主要借助于操作系统提供的集群软件来实现，可以采用单活或者双活方式。

数据库应用一级的高可用性集群，主要借助于数据库管理系统软件提供的应用集群软件实现，常用的数据管理系统产品中，SQL Server 主要采用单活模式，Oracle 主要采用双活模式。

各类应用服务软件一级的高可用集群，主要借助于应用软件提供的集群软件实现。

2.5.5　广域网技术选择与应用

2.5.5.1　城域网远程接入技术

随着网络，尤其是企业网络规模的不断发展，网络用户的流动性和地域分散特性不断增加。远程企业用户需要借助于特殊的接入方式实现对企业网络的访问，而城市的网络用户也需要借助于同样的技术来实现对互联网络的访问，因此这些特殊的技术主要应用于城域网络，可以被称为“城域网远程接入技术”。

1. 传统的 PSTN 接入技术

PSTN 接入技术是较为经典的远程连接技术，通过在客户计算机和远程的拨号服务器之间分别安装调制解调器，实现数字信号在模拟语音信道上的调制，通过公用电话网（PSTN）完成数据传输。

PSTN 接入的传输速率较低，目前常见的速率是 33.6Kbps 或者 56Kbps；其中 33.6Kbps 双向传输速率相同，而 56Kbps 的双向传输速率不均衡，上行为 33.6Kbps，下行为 56Kbps；同时，PSTN 的接入速率还要受调制解调器性能和电话线路质量的影响。

PSTN 接入技术主要使用两种协议，分别为 PPP 和 SLIP，其中 SLIP 只能为 TCP/IP 协议提供传输通道，而 PPP 可以为多种网络协议族提供传输通道，因此 PPP 协议也是应用最广的协议。

设计 PPP 协议时需要考虑到口令认证机制，PPP 协议支持两种类型的认证机制，分别为口令认证协议（PAP）和应答握手认证协议（CHAP）。其中，PAP 协议在进行认证时，用户的口令以明文方式进行传递，而 CHAP 则利用三次握手和一个临时产生的可变应答值来验证远程节点，因此在实际应用中，应尽量使用 CHAP 作为 PPP 协议的认证机制。

在设计 PSTN 接入时，需要在网络中添加远程访问服务器（RAS），通常都是带有拨号服务功能的路由器；这些路由器可以配置内置 Modem 的拨号模块，也可以通过普通模块连接外置 Modem 池实现，RAS 除了可以在自身存储静态的用户名和密码之外，还可以借助于 RADIUS、TACACS 等服务完成对动态用户与口令库的访问，如图 2-55

所示。

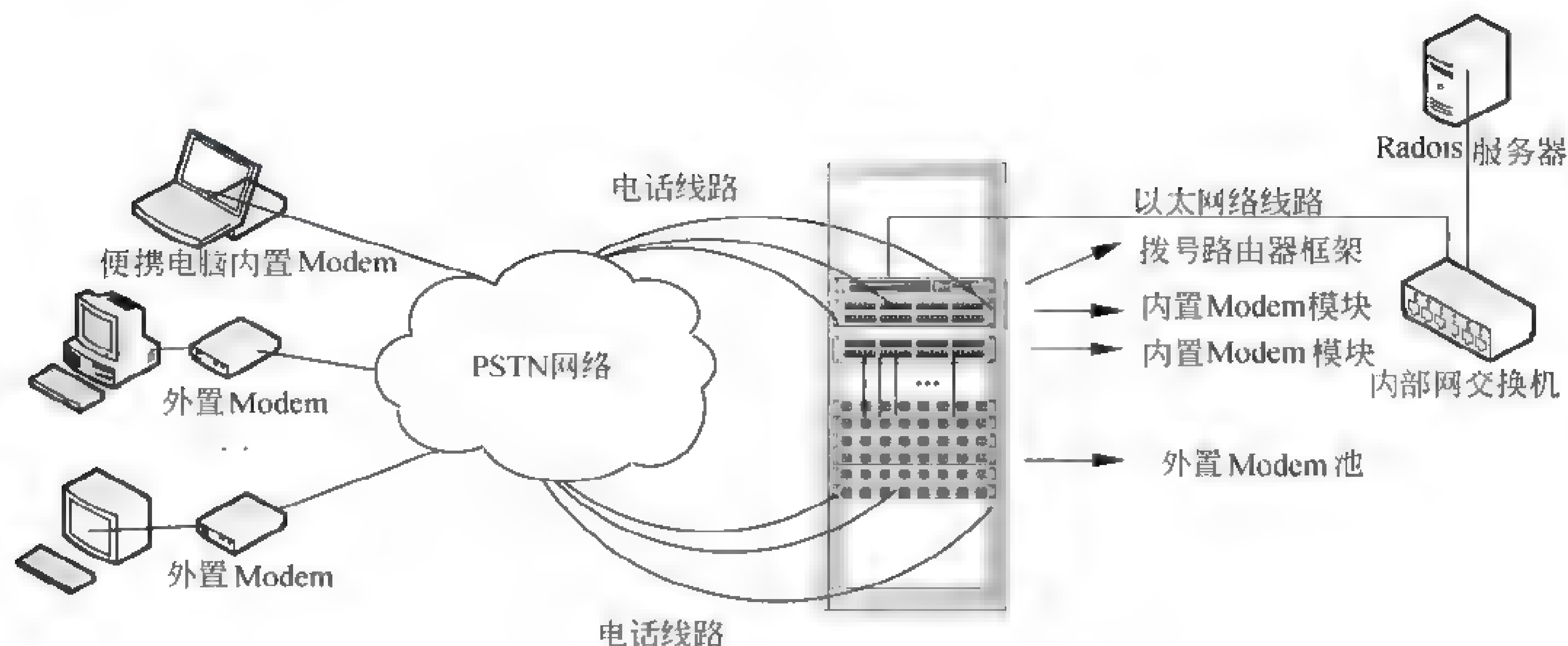


图 2-55 PSTN 接入

2．综合业务数据网

综合业务数据网（ISDN）是由地区电话服务提供商提供的数字数据传输业务，支持在电话线上传输文本、图像、视频、音乐、语音和其他的媒体数据，ISDN 上使用 PPP 协议，以实现数据封装、链路控制、口令认证、协议加载等功能。

ISDN 提供的电路包括 64Kbps 的承载用户信息信道（B 信道）和承载控制信息信道（D 信道），同时 ISDN 提供了两种用户接口，分别为基本速率接口和基群速率接口。

- 基本速率接口（Basic Rate Interface，BRI）——包含两个 B 信道和一个 16Kbps 的 D 信道。
- 基群速率接口（Primary Rate Interface，PRI）——包含 30 个 B 信道和一个 64Kbps 的 D 信道。

基本速率接口主要用于个人用户的远程接入，而基群速率接口主要用于企业或者团体的接入，如图 2-56 所示。个人接入中，通过运营商端 ISDN 交换机提供的接口，实现计算机信号和语音信号的分离，计算机信号通过 PRI 接口经路由器进入网络；在企业接入中，两端的路由器通过带有 PRI 接口的路由器互连，完成了两个网络的连接。

3．电缆调制解调器远程接入

电缆调制解调器运行在有线电视（CATV）使用的铜轴电缆上，可以提供比传统电话线更高的传输速率，典型的电缆网络系统提供 25～50Mbps 的下行带宽和 2～3Mbps 的上行带宽，同时电缆调制解调器的另一个优势是不需要拨号就能实现远程站点访问。

电缆调制解调器需要对传统的单向 CATV 网络进行双向改造形成数字电缆业务网络，可以采用双缆方式（一根上行、一根下行）和单缆方式（高频下行、低频上行）。运

营商通常采用混合光纤 / 铜缆（Hybrid Fiber/Coax，HFC）系统将 CATV 网络和运营商的高速光纤网络连接在一起。HFC 系统使用户能将计算机或者小型局域网连接到用户的铜轴电缆上，高速地访问因特网或使用 VPN 软件接入到企业网络。

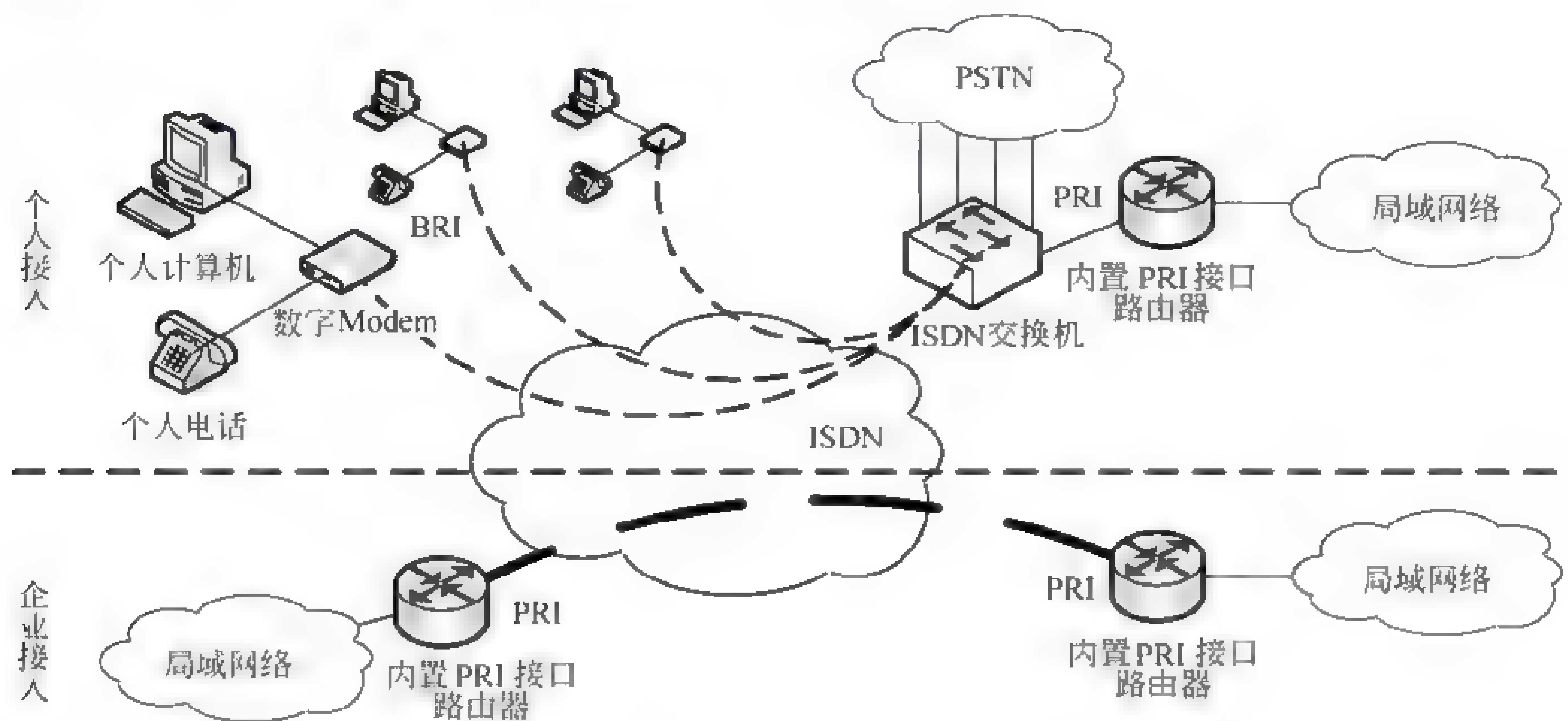


图 2-56　ISDN 接入

使用电缆调制解调器远程接入必须依赖于运营商一端的电缆调制解调器终结设备（CMTS），该设备向大量的电缆调制解调器提供高速连接；多数运营商都会借助于通用的宽带路由器来实现 CMTS 功能，这些路由器安装在运营商的电缆服务头端，同时提供计算机网络和 PSTN 网络的连接。

如图 2-57 所示，CMTS 的以太口可以直接与以太网相连，同时通过中继线路连接 PSTN 网络，将双向的网络和语音信号调制形成上行和下行的模拟信号，单向的有线电视下行信号以频分复用合入下行信号中；在 HFC 区域中，借助于光收发器、光电转换器等设备完成信号的中继和传递，通常光纤采用双纤而电缆采用单缆；客户端采用 Cable Modem 相连，并分解出有线电视、计算机网络和电话信号。

4．数字用户线路远程接入

数字用户线路（Digital Subscriber Line，DSL）允许用户在传统的电话线上提供高速的数据传输，用户计算机借助于 DSL 调制解调器连接到电话线上，通过 DSL 连接访问互联网络或者企业网络。

DSL 采用尖端的数字调制技术，可以提供比 ISDN 快得多的速率，其实际速率取决于 DSL 的业务类型和很多物理层因素，例如电话线的长度、线径、串扰和噪音等。

DSL 技术存在多种类型，常见的技术类型如下。

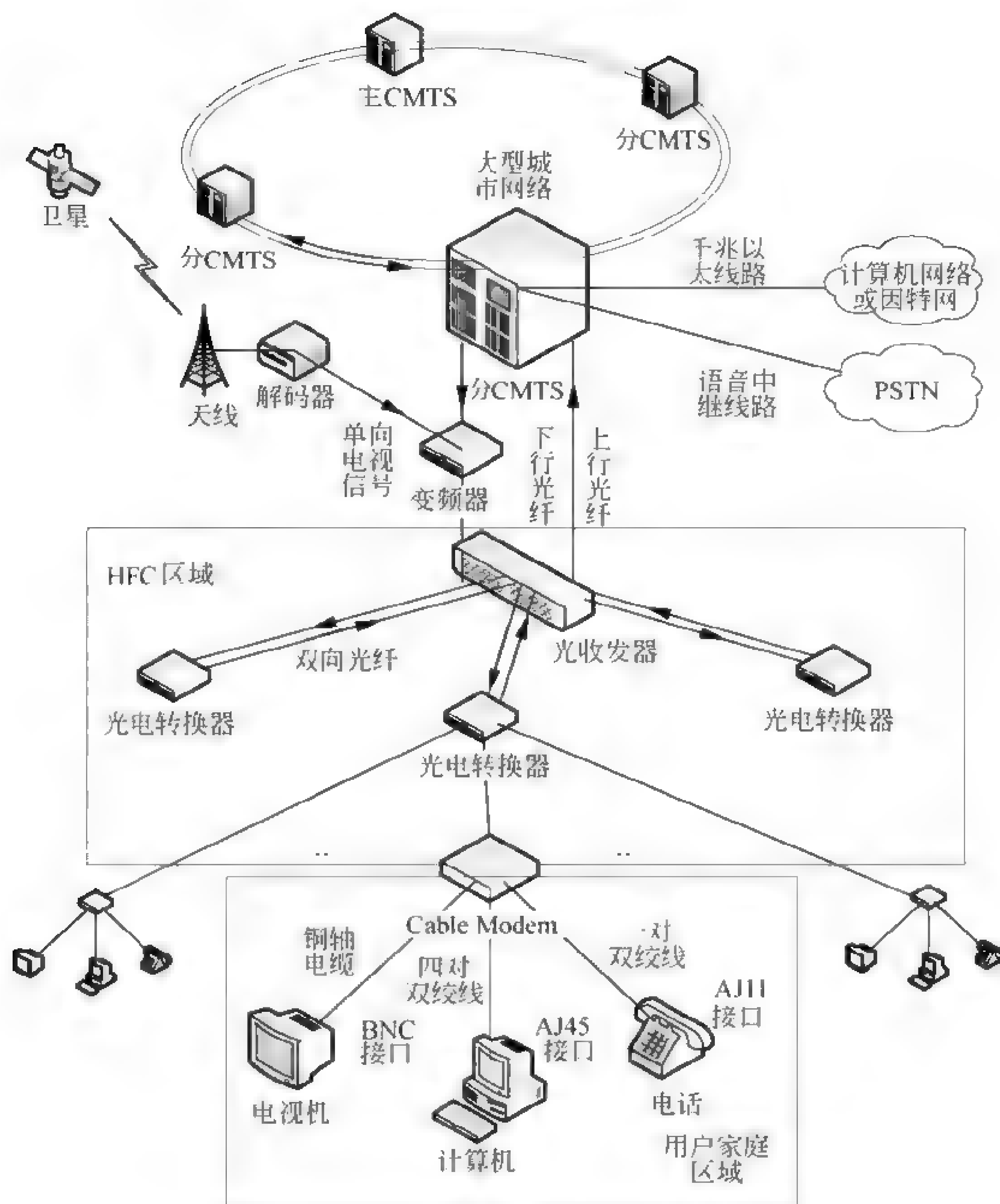


图 2-57 电缆调制解调器远程接入

- ADSL：非对称 DSL，用户的上下行流量不对称，一般具有三个信道，分别为 1.544～9Mbps 的高速下行信道、16～640Kbps 的双工信道、64Kbps 的语音信道。
- SDSL：对称 DSL，用户的上下行流量对等，最高可以达到 1.544Mbps。
- ISDN DSL：介于 ISDN 和 DSL 之间，可以提供最远距离为 4600～5500m 的 128Kbps 双向对称传输。
- HDSL：高比特率 DSL，是在两个线对上提供 1.544Mbps 或在三个线对上提供 2.048Mbps 对称通信的技术，其最大特点是可以运行在低质量线路上，最大距离为 3700～4600m。

- VDSL：甚高比特率 DSL，一种快速非对称 DSL 业务，可以在一对电话线上提供数据和语音业务。

在这些技术中，ADSL 的应用范围最广，已经成为城域网接入的主要技术。

ADSL 接入需要的设备包括接入设备（局端设备 DSLAM 和用户端设备 ATU-R）、用户线路和管理服务器。其中 DSLAM 作为 ADSL 的局端收发传送设备，主要由运营商提供，为 ADSL 用户端提供接入和集中复用功能，同时提供不对称数据流的流量控制，用户可以通过 DSLAM 接入到 IP 等数据网和传统的语音电话网；用户端设备 ATU-R，实现 POTS 语音与数据的分离，完成用户端 ADSL 数据的接收和发送，即 ADSL Modem；ADSL 采用双绞线作为承载媒质，语音与数据信号同时承载在双绞线上，无须对现有的用户线路进行改造，有利于宽带业务的开拓；管理服务器主要是宽带接入服务器（BRAS），除了能够提供 ADSL 用户接入的终结、认证、计费、管理等基本 BRAS 业务，还可以提供防火墙、安全控制、NAT 转换、带宽管理、流量控制等网络业务管理功能，如图 2-58 所示。

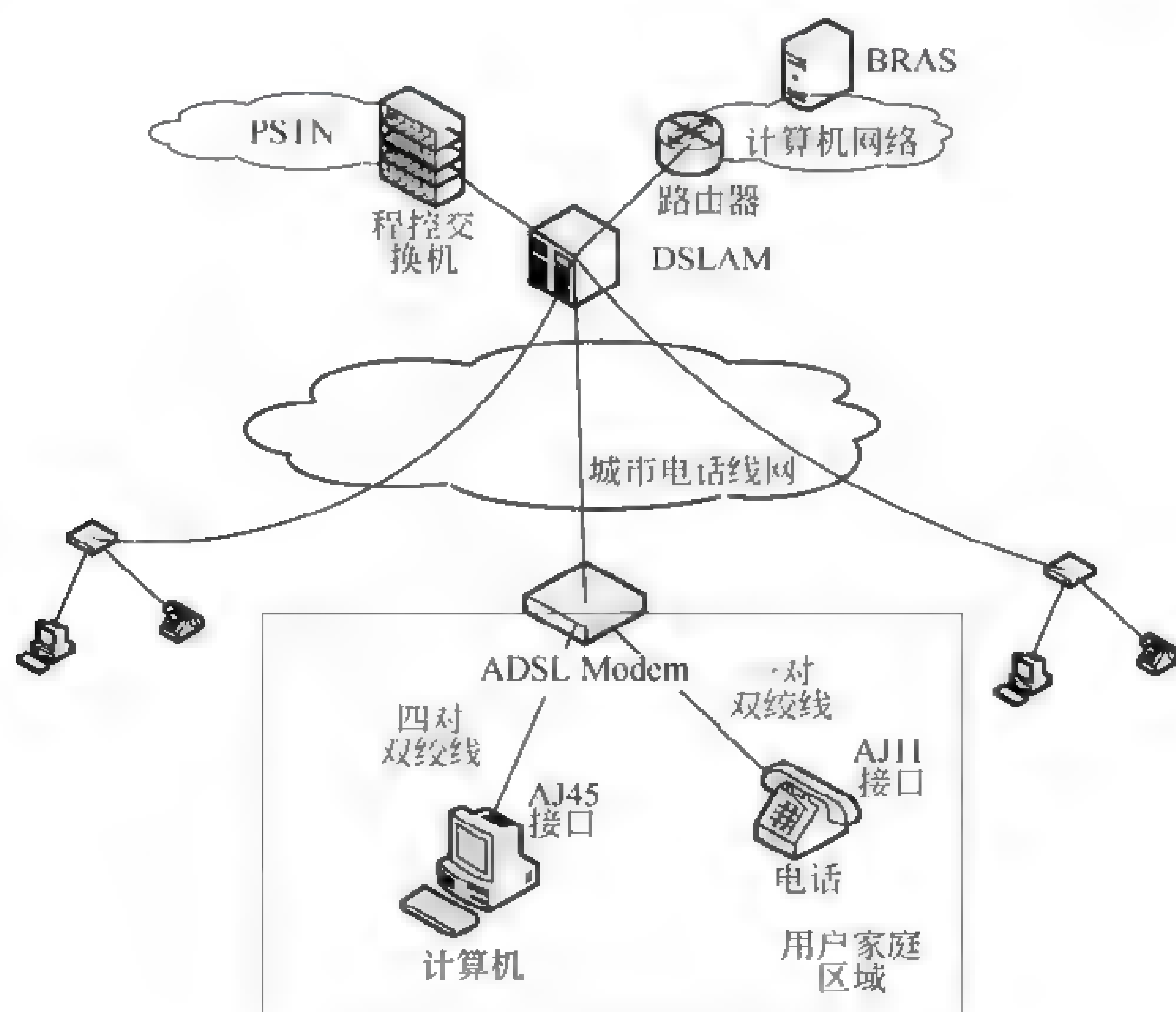


图 2-58　ADSL 接入

在选择城域网远程接入技术时，主要是依据现有城域网的建设情况，并适当考虑租用经费；一般来说，城域网的远程接入主要是由电信运营商提供，设计人员需要根据远程用户的分布、用户是否需要形成专用网络、运营商的线路铺设、租赁费用等情况，与电信运营商技术服务人员进行协商和讨论，形成最终接入方案。

2.5.5.2 广域网互连技术

1．数字数据网络

数字数据网络（Digital Data Network，DDN）是一种利用数字信道提供数据信号传输的数据传输网，是一个半永久性连接电路的公共数字数据传输网络，为用户是供了一个高质量、高带宽的数字传输通道。

DDN 采用同步时分复用，对各层协议透明，因此 DDN 支持任何的传输规程；DDN 不具备交换功能，以点对点方式实现半永久性的电路连接，传输延时小；DDN 采用数字信道传输数据信号，与传输的模拟信号相比，具有传输质量高、速度快、带宽利用率高等优点；DDN 的传输安全可靠，由于采用多路由的网状拓扑结构，单个节点的失效不会导致整个线路的中断。

DDN 网络实行分级管理，其网络结构按网络的组建、运营、管理、维护的责任地理区域，可以分为一级干线网、二级干线网和本地网三级。一级干线网由设置在各省、自治区和直辖市的节点组成，二级干线网由设置在省内的节点组成，本地网是指城市范围内的网络，由这些网络提供全国范围内的电路连接服务。

利用 DDN 网络实现局域网互联时，必须借助于路由器和 DDN 网络提供的数据终端设备 DTU；DTU 其实是 DDN 专线的调制解调器，直接和 DDN 网络通过专线连接，如图 2-59 所示。



图 2-59 利用 DDN 实现局域网互联

DDN 网络可以为两个终端用户网络之间提供带宽最低为 9.6Kbps，最高为 2Mbps 的数据业务，虽然面临各种新型传输技术的挑战，但由于 DDN 可以为任何信号和传输协议提供透明传递，迄今为止 DDN 仍在广域网互联技术应用中占据一席之地。

2．SDH

SDH（Synchronous Digital Hierarchy，同步数字体系）是一种将复接、线路传输及交换功能融为一体，并由统一网管系统操作的综合信息传送网络，前身是美国贝尔通信技术研究所提出来的同步光网络（SONET）。SDH 可实现网络有效管理、实时业务监控、动态网络维护、不同厂商设备间的互通等多项功能，能大大提高网络资源利用率、降低

管理及维护费用、实现灵活可靠和高效的网络运行与维护，因此也是当前最主要的运营商基础设施网络。

SDH 网络是基于光纤的同步数字传输网络，采用分组交换和时分复用（TDM）技术，主要由光纤和挂接在光纤上的分插复用器（ADM）、数字交叉连接（DXC）、光用户环路载波系统（OLC）构成网络的主体，整个网络中的设备由高准确度的主时钟统一控制。SDH 网络基本的运行载体是双向运行的光纤环路，可根据需要采用单环、双环或者多环结构，SDH 支持多种网络拓扑结构，组网方式非常灵活，如图 2-60 所示。

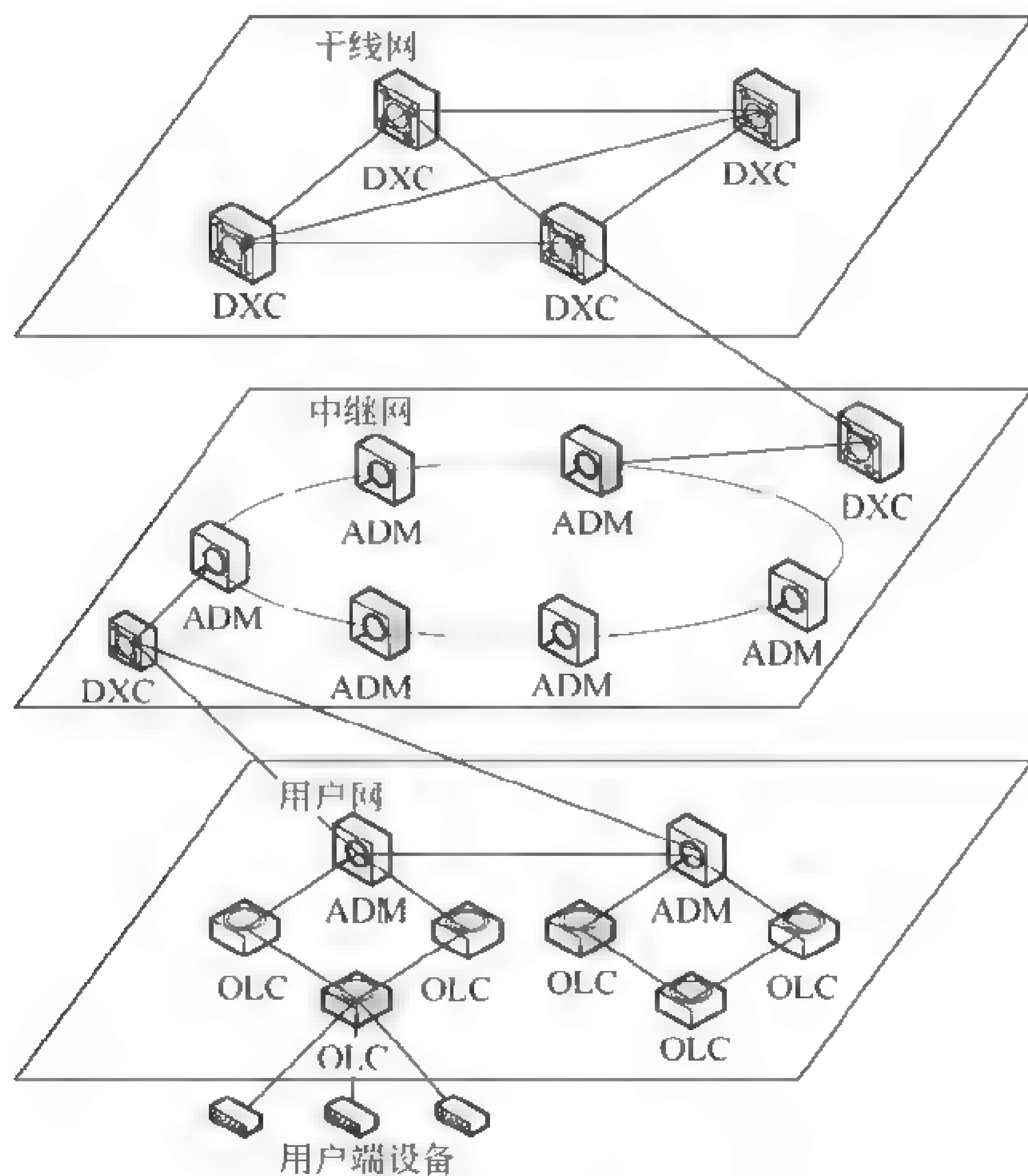


图 2-60　SDH 网络结构

SDH 采用的信息结构等级称为同步传送模块 STM-N（Synchronous Transport，N=1，4，16，64），最基本的模块为 STM-1，4 个 STM-1 同步复用构成 STM-4，16 个 STM-1 或 4 个 STM-4 同步复用构成 STM-16；STM-1 的传输速率为 155.520Mbps，而 STM-4 的传输速率为 4×155.520=622.080Mbps，STM-16 的传输速率为 16×155.520=2488.320Mbps，并依此类推；SDH 同时也可以提供 E1、E3 等传统传输速率服务。

SDH 是主要的广域网互联技术，利用运营商的 SDH 网络实现互联，可以采用两种方式，分别是 IP over SDH 和 PDH 兼容方式。

IP over SDH：以 SDH 网络作为 IP 数据网络的物理传输网络，并使用链路适配及成

帧协议（PPP）对 IP 数据包进行封装，然后按字节同步的方式把封装后的 IP 数据包映射到 SDH 的同步净荷封装中进行连续传输。IP over SDH 为 IP 网络设备提供的接口主要是 POS（Packet Over SONET/SDH）接口，该接口可以提供 STM-1 及其以上的传输速率。

准同步数字系列（Plesiochronous Digital Hierarchy，PDH）兼容方式：由于单纯的 SDH 网络只能提供 STM-1 以上的传输速率，而大多数用户并不需要这么高的数据传输速率，因此 SDH 提供了对传统 PDH 的兼容方式；这种方式在 SDH 中的最低速率同步传输模块 STM-1 中封装了 63 个 E1 信道，可以最多同时向 63 个用户提供 2Mbps 的接入速率。PDH 兼容方式可以提供两种方式的接口：一是传统 E1 接口，例如路由器上的 G.703 转 V35 接口；另外是封装了多个 E1 信道的 CPOS（Channel POS），路由器通过一个 CPOS 接口接入 SDH 网络，并通过封装的 E1 信道连接多个远程站点。

以上借助于 SDH 网络实现局域网络互联的各种方式如图 2-61 所示。

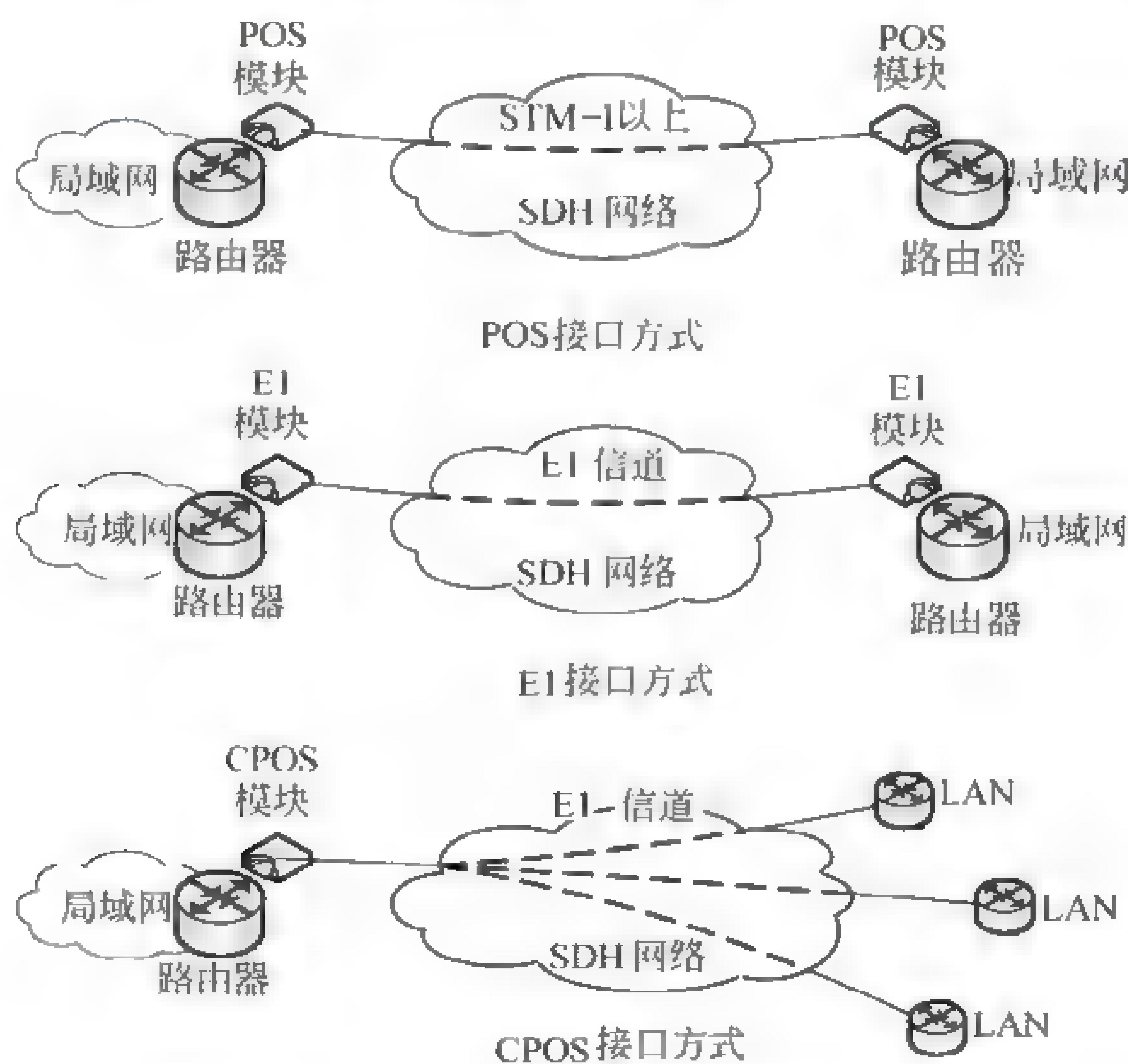


图 2-61 利用 SDH 网络实现局域网互联

无论是 IP over SDH 方式还是 PDH 兼容方式，运营商都可以将线路转换成以太网络链路，以便于向用户提供应用更为普遍、成本更加低廉的以太网络接口；其中较为常见的是将多条 E1 信道转换成为以太网，例如两个局域网络之间通过 4 条 E1 信道互联，客户端的光端机或者转换设备将 4 条 E1 信道转换成十兆的以太网线路，如图 2-62 所示。

3．MSTP

由于具有可靠的业务保护能力，SDH 技术已经成为城域传输网的一种经典选择，但

是 SDH 也存在包括带宽瓶颈、多层网络结构指配过于复杂以及支持业务单一等诸多问题，尤其是对可变速率业务的支持方面；对于固定速率的业务（如传统话音业务），SDH 很容易将其适配到固定容量通道中，但对于可变速率 VBR 业务和任意速率业务，SDH 则显得不够灵活，特别是传送效率不高；欧洲、东亚及印度的一些运营商已经在新建网络（特别是城域网）中完全摒弃 SDH 技术体系；但是目前国内的 SDH 网络已经庞大得让传统的电信运营商无法从容、坦然地弃之而去，因此被称为下一代 SDH 的 MSTP 应运而生。

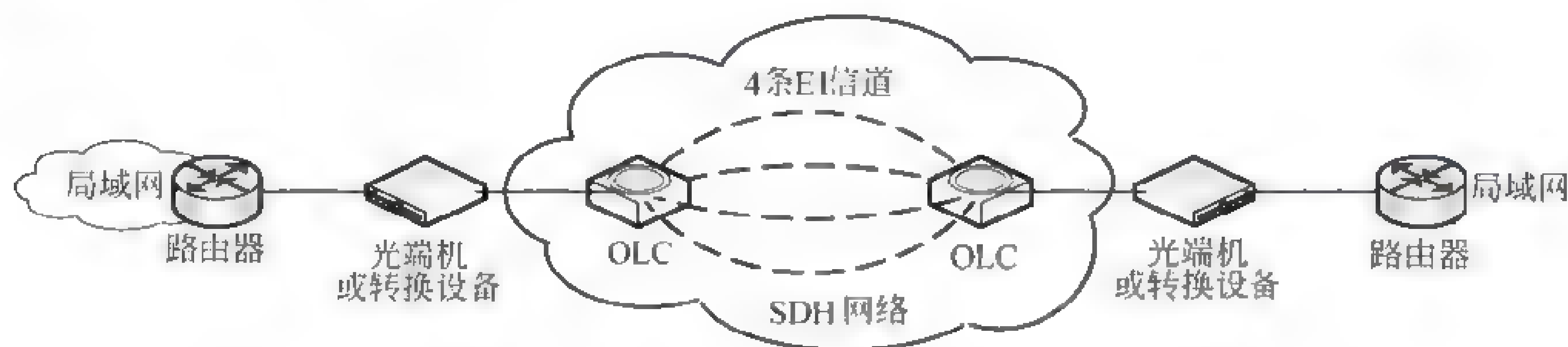


图 2-62　SDH 与以太网转换

基于 SDH 的多业务传送平台（MSTP）是指基于 SDH 平台同时实现 TDM、ATM、以太网等业务的接入、处理和传送，提供统一网管的多业务节点。基于 SDH 的多业务传送节点除应具有标准 SDH 传送节点所具有的功能外，还具有以下主要功能特征：

- 具有 TDM 业务、ATM 业务或以太网业务的接入功能。
- 具有 TDM 业务、ATM 业务或以太网业务的传送功能包括点到点的透明传送功能。
- 具有 ATM 业务或以太网业务的带宽统计复用功能。
- 具有 ATM 业务或以太网业务映射到 SDH 虚容器的指配功能。

MSTP 在网络互联领域主要用于企业用户网络建设和用户接入补充，其中企业用户网络建设直接体现了 MSTP 多种业务接入、点到多点的透明传送功能。企业客户网络数量较多，地点分布零散，业务需求各不相同，如果把所有企业专网纳入统一的 SDH 传输平台，则投资成本过高。可针对企业网络业务的种类、数量并考虑到服务等级、投资成本等因素，分期、分层对企业网络进行优化、改造，在部分企业专网中引入 MSTP 设备，采用环型和星型网络拓扑结合的方式，逐步实现对不同等级客户的不同服务质量保障。MSTP 平台可以提供 SDH 网络提供的所有传输带宽，并且能够实现多个网络部分之间共享传输带宽。

具体的建设方案如下：将企业网络服务平台划分为核心层和接入层，将业务发展良好、业务集中、业务种类复杂的企业专网和重点企业用户纳入核心层。通过对光缆线路资源进行优化，在核心层引入 MSTP 设备组成环网，建立专有的重要企业业务平台，提供丰富的业务种类和可定制服务（ATM、Ethernet 以及 2M 专线等业务），网络的结构、容量、管理和发展均以满足重点企业业务的开展为基准；将业务数量少、业务种类较单

一、节点多且分布零散的企业分支机构及小型企业纳入接入层，出于成本考虑，接入层仍保持星型组网或光纤直连方式，今后可根据客户业务的发展，逐步进行改造。

图 2-63 是利用 MSTP 技术，实现一个企业不同局域网络之间连接的示例。MSTP 设备借助于 SDH 网络提供的链路，形成 MSTP 业务环，企业的不同局域网借助于路由器接入到 MSTP 设备的以太网接口；这些企业网络所有的局域网之间的连接并不需要占用多个 SDH 信道，而是共享一个传统 SDH 信道的带宽，通过这种方式，可以避免企业网络连接对 SDH 网络资源的大量浪费；同时由于各个局域网络之间访问的透明性、随机性和不确定性，企业用户的网络感受和传统 SDH 互联方式区别不大。

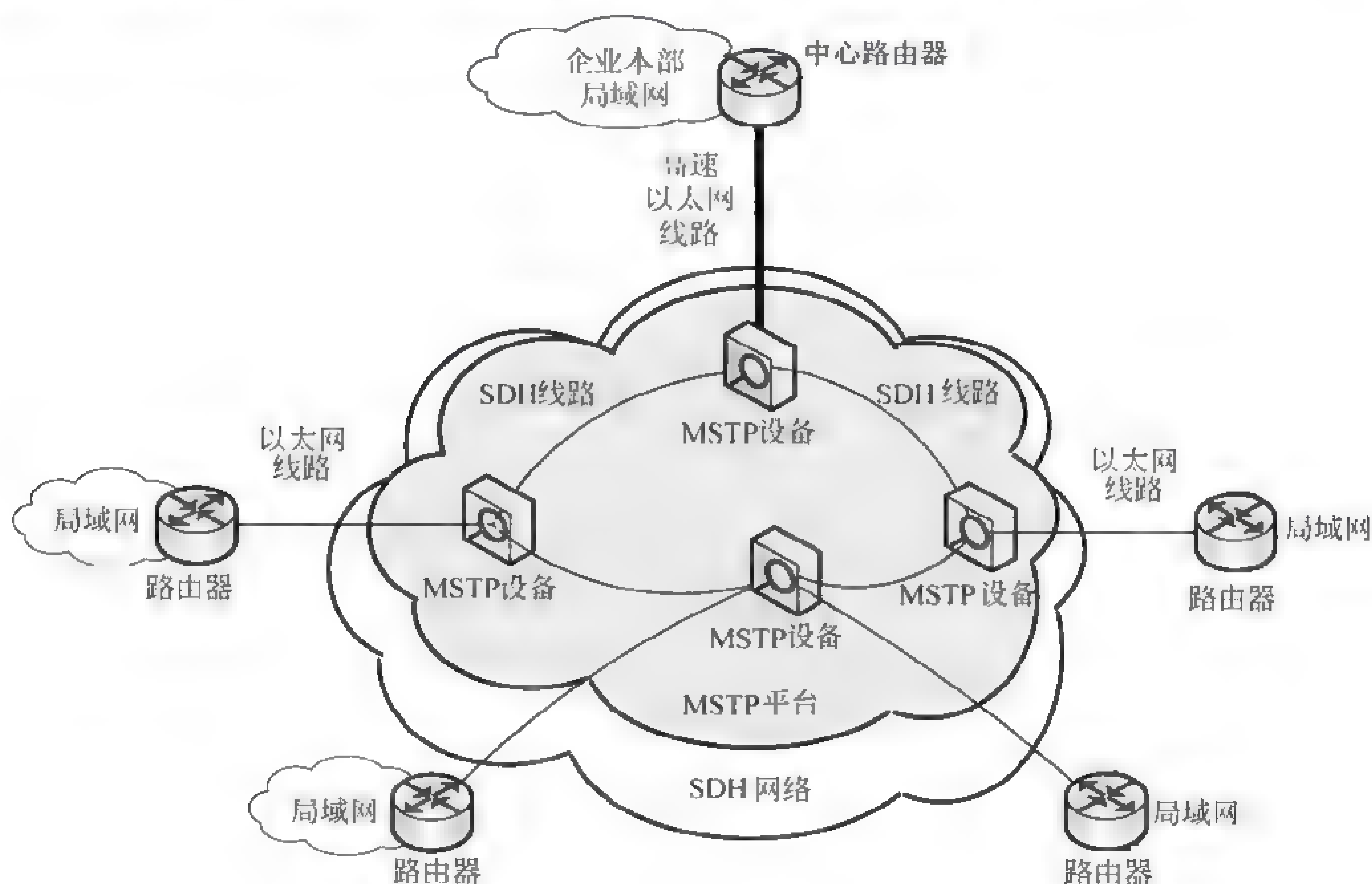


图 2-63　利用 MSTP 平台实现局域网互联

4．传统 VPN 技术

虚拟专用网（VPN）通过公共网络实现远程用户或远程局域网之间的互联，主要采用隧道技术，让报文通过如 Internet 或其他商用网络等公共网络进行传输。由于隧道是专用的，使得通过公共网络的专用隧道进行报文传输的过程和通过专用的点对点链路进行报文传输的过程非常相似，由于公共网络可以同时具有多条专用隧道，因而就可以同时实现多组点对点报文传输。

传统的 VPN 技术主要基于实现数据安全传输的协议来完成，主要包括两个层次的数据安全传输协议，分别为二层协议和三层协议。二层协议主要是对传统拨号协议 PPP 的扩展，通过定义多协议跨越第二层点对点连接的一个封装机制，来整合多协议拨号服

务至现有的因特网服务提供商点，保证分散的远程客户端通过隧道方式经由 Internet 等网络访问企业内部网络；其典型协议为 L2TP，主要用于利用拨号系统实现远程用户安全接入企业网络；三层协议主要定义了在一种网络层协议上封装另一个协议的规范，通过对需要传递的业务数据的网络层分组进行封装，封装后的分组仍然是一个网络层分组，可以在 VPN 寄生的网络上进行传递，使得各个 VPN 部分之间可以借助于隧道进行通信；典型的三层协议包括 IPSec 和 GRE，其中 IPSec 主要是在 IP 协议上实现封装，GRE 是一种规范，可以适用于多种协议的封装。

基于三层协议的 VPN 技术主要用于企业各局域网络之间的连接，分为点对点方式和中心辐射状方式，如图 2-64 所示。点对点方式（point-to-point）下，两个分支局域网络边界上部署 VPN 网关或者是带有 VPN 功能的防火墙、路由器，这些 VPN 网关通过物理链路接入互联网，并由 IPSec 协议或 GRE 协议形成两个路由器之间的逻辑隧道，实现局域网络之间的数据传递；中心辐射状方式（hub-and-spoke）下，核心局域网和各分支局域网的边界上都部署 VPN 网关，核心局域网路由器和每个分支局域网路由器之间建立逻辑隧道，完成多个局域网分支的互连，分支局域网之间的访问需要经过中心局域网的转发。

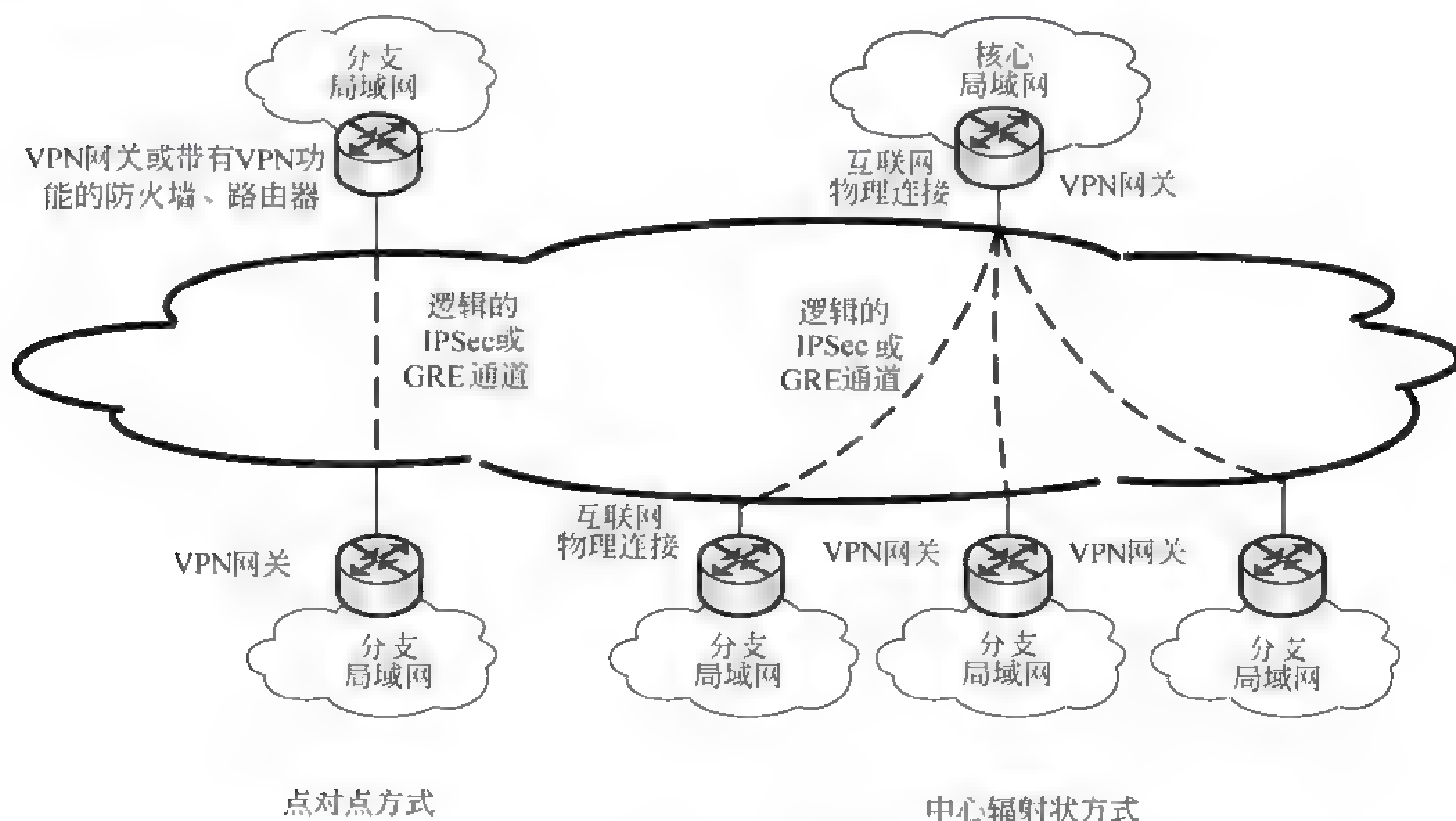


图 2-64 利用三层 VPN 技术实现局域网络互联

5. MPLS VPN 技术

MPLS 是多协议标签交换的简称，它用短而定长的标签来封装分组。MPLS 从各种链路层（如 PPP、ATM、帧中继、以太网等）得到链路层服务，又为网络层提供面向连接的服务。MPLS 能从 IP 路由协议和控制协议中得到支持，同时还支持基于策略的约

束路由，路由功能强大、灵活，可以满足各种新应用对网络的要求。

MPLS 技术主要是为了提高路由器转发速度而提出的，其核心思想是利用标签交换取代复杂的路由运算和路由交换；该技术实现的核心就是在 IP 数据包之外封装一个 32 比特的 MPLS 包头，如图 2-65 所示；MPLS 体系中的各个路由设备，将根据 MPLS 包头中的标签进行转发，而不是传统方式下根据 IP 包头中的目标地址来转发；由于 MPLS 标签栈可以无限嵌套，从而提供无限的业务支持能力，而 MPLS VPN 就是一个典型的标签嵌套应用。



图 2-65 MPLS 封装

MPLS VPN 是一种基于 MPLS 技术的 IP-VPN，是在网络路由和交换设备上应用 MPLS 技术，简化核心路由器的路由选择方式，利用结合传统路由技术的标记交换实现的 IP 虚拟专用网络（IP VPN），可用来构造合适宽带的企业网络、专用网络，满足多种灵活的业务需求。采用 MPLS VPN 技术可以把现有的 IP 网络分解成逻辑上隔离的网络，这种逻辑上隔离的网络的应用可用在解决企业互连、政府相同/不同部门的互连，也可以用来提供新的业务，为解决 IP 网络地址不足、QoS 需求、专用网络等需求提供较好的解决途径，因此也成为新型电信运营商提供局域网络互联服务的主要手段。

一个典型的 MPLS VPN 承载平台如图 2-66 所示。

承载平台上的设备主要由各类路由器组成，这些路由器在 MPLS VPN 平台中的角色各不相同，分别被称为 P 设备、PE 设备、CE 设备；P 路由器（provider router）是 MPLS 核心网中的路由器，这些路由器只负责依据 MPLS 标签完成数据包的高速转发；PE 路由器（Provider Edge Router）是 MPLS 核心网上的边缘路由器，与用户的 CE 路由器互连，PE 设备负责待传送数据包的 MPLS 标签的生成和弹出，负责将数据包按标签发送给 P 路由器或接收来自 P 路由器的含标签数据包，PE 路由器还将发起根据路由建立交换标签的动作；CE（Custom Edge）路由器是直接与电信运营商相连的用户端路由器，该设备上不存在任何带有标签的数据包，CE 路由器将用户网络的信息发送给 PE 路由器，以便于在 MPLS 平台上进行路由信息的处理。

如图 2-66 所示，一个企业可以借助于 MPLS VPN 承载平台，将由不同 CE 路由器互连的局域网络互联起来形成一个完整的企业网络；在这个 MPLS VPN 平台上，可以存在多个企业网络，这些网络之间除非特殊设置，相互之间是逻辑隔离的，不同企业网络之间不能直接互访；用户网络只需要提供 CE 路由器，并连接到 PE 路由器，由平台管

理员完成 VPN 的互连工作；PE 路由器可以同时和多个 CE 路由器建立物理连接，也可以借助于支持 MPLS 协议的交换机，通过 VLAN 技术实现和多个 CE 路由器的互连，从而保证多个用户网络部分的接入。

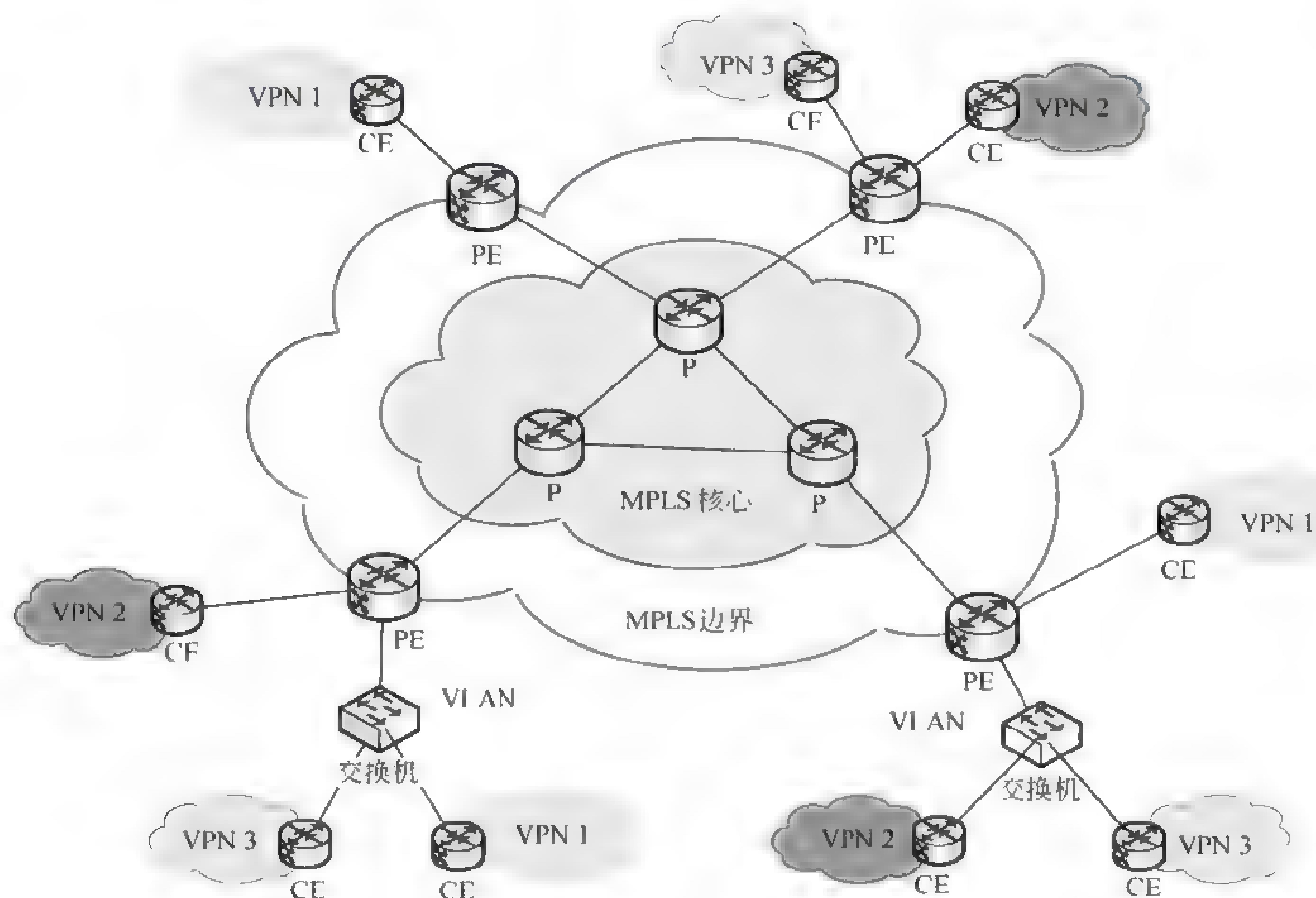


图 2-66 MPLS VPN 承载平台

2.5.5.3 广域网性能优化

广域网连接的可靠性和可伸缩性将决定企业内部网是否有效地满足用户的需要，通过广域网络优化，可以分析企业通信网络的所有组成部分，并确定如何进行优化，以提高总体性能并降低综合费用。

对于广域网性能的优化，可以从以下方面进行考虑。

1．广域网网络瓶颈

在企业内部网中，无论各个局域网络内部的带宽是如何的冗余，一旦各局域网络的广域网连接不能提供局域网互访的带宽需求，都会形成企业网络的瓶颈，会严重影响企业网络的整体性能。

因此，在进行逻辑设计时，应在保证总体投资不超过预算的同时，尽量提升广域网络的带宽；另外，当借助于广域网将各局域网互联起来后，可以对这些网络之间的互访

设计较为严格的访问控制策略，只允许必要的通信流量，提供对广域网带宽的合理利用和分配。

2．利用路由器实现广域网预留带宽

路由器不是实现局域网络互联的唯一设备，代理服务器、应用网关等设备也都可以实现各局域网络的互联，只是互联的层次不同，由于路由器工作在网络层，并且具有一些针对信息流的优化措施，因此应尽量使用路由器来完成局域网互联，这些优化措施包括以下一些内容：

- 路由器可过滤不必要的局域网通信量，包括广播通信流量，不支持路由协议的通信和发向未知网络的信息等。
- 路由器拥有较强的数据包检查、验证机制，并可以通过数据包的优先级别、队列机制等，对网络流量进行优化。
- 路由器可以针对不同的广域网技术，对各类协议参数进行优化，通过不断调整参数，达到整体网络性能的优化。
- 路由器可以将各类错误的影响限制在一个特定的区域内，限制了错误的影响范围。

3．拨号线路的应用

拨号线路虽然提供的广域网带宽较低，相对来说稳定性较差，但是在减少广域网网络成本和提供后援备份电话线方面有其突出的优势。

可以在以下的情况考虑使用拨号线路，对现有广域网络进行优化。

网络中存在大量分散的用户，这些用户对网络的访问需求是不固定的，并且通常访问网络所产生的流量较少，通过拨号线路的应用，可以避免远程用户在不访问网络时广域网络线路资源的占用，仅利用少量线路满足大量用户的远程访问需求，在保证网络访问的同时降低网络建设成本。

路由器等设备在正常线路之外，可以将拨号线路作为附件带宽线路；一旦产生拥塞，则可以启动拨号线路来增加带宽。

拨号线路也是经济实惠的备用线路，在正常情况下，拨号线路不启用，不会产生流量费用；当检测到故障产生时，广域网络设备可以启动拨号线路，建立备份路径，保证网络的正常通信。

4．压缩

采用数据压缩技术可以有效利用较小的广域网络带宽，这些压缩技术主要由广域网络中的路由器实现，实现数据传输压缩的方式主要有两种，分别是基于历史数据的压缩和所有数据包压缩。

基于历史数据的压缩——该类压缩模式中，路由设备从多个数据包中找出重复的数据模式，使用更短的代码进行替代，发送方和接收方都有加密模式和密码词典，同时也可以实现数据包的加密和解密。为了避免数据丢失对后续压缩数据的影响，基于历史数

据的压缩技术必须应用在较为可靠的数据链路上。

所有数据包压缩——该类模式对所有数据包都进行重复查找，并使用更短的代码进行替换，每个压缩后的数据包都是独立的压缩体，可以自行进行解压操作，由于单个数据包丢失不会对其他数据包造成影响，因此该类压缩技术可以运行在不可靠的数据链路上。

5. 链路聚合

当路由器上的一个广域网连接提供的带宽不能满足应用需求时，网络管理可以考虑申请多个广域网链路，并且将这些链路聚合成一个虚拟的链路，从而实现对广域网络的优化，例如在使用 SDH 网络完成局域网互联时，路由器上的广域网接口只能和一条 E1 信道连接，提供 2 兆的带宽，网络管理员可以申请多条 E1 线路，利用路由器上的冗余广域网端口连接 E1 线路，同时将多条链路聚合成一个逻辑连接，这样可以为广域网提供多个 E1 信道的传输带宽，而同时不需要修改路由的相关配置。

6. 数据优先排序

数据包的优先权排序赋予管理员更多的灵活性，管理员可赋予传输队列中对时间敏感消息更高的优先权，保证这些数据的优先发送和溢出保护。通常优先权方案为每个数据包分配确定的优先权，然后按紧急、高级、一般和低级 4 个级别为数据包赋予 4 个优先权队列之一。

网络关键信息（如有关拓扑结构改变的路由协议更新）自动被分配到紧急优先权队列中，紧急数据包在所有信息中具有最高优先权。紧急优先权队列中所有的数据包发送完以后，路由器再按照用户配置参数控制的顺序向广域网接口发送其他队列的数据包。

7. 协议带宽预留

协议带宽预留可以让管理员为特殊的协议和应用按比例分配带宽，例如，网络管理员可以将广域网总带宽的 10%分配给 HTTP 协议，10%分配给 FTP 协议，20%分配给 SMTP 和 POP3 协议，其余的带宽不做分配。

协议带宽预留不同于数据优先权排序的方案，主要是根据协议的类型进行带宽预留约定；例如，当广域网络带宽的 10%预留给 HTTP 协议时，即使网络设备上还存在较高优先权的数据包需要发送，只要 HTTP 协议数据占据了 10%的带宽，这些高优先权的数据也不能占用 HTTP 的带宽；而预留的另外一个意思是，如果这些预留的带宽特定协议使用不了，则可以由其他协议占用。

8. 对话公平

对话公平是对协议预留方案的增强，它保证通信平等地在所有用户间传输，不允许某个用户垄断广域网带宽。对话公平主要是为了防止一些用户长期占用网络资源，而影响了其他用户的网络访问，对话公平在协议带宽预留的基础上，将预留的网络带宽平均分配给所有的协议用户，例如总带宽的 10%被分配给了 HTTP 协议，而当前有 20 个 HTTP 对话连接，则每个连接的带宽都将被限制为 HTTP 协议预留带宽的 1/20，也就是总带宽

的 5%，这样可以保证每个 HTTP 用户都能够均衡地访问网络。

2.5.6 地址设计和命名模型

2.5.6.1 分配网络层地址的原则

分配规划、管理和记录网络层地址是网络管理工作的重点内容，好的网络层地址分配规划，不仅可以让管理员对地址实施便捷的管理，也为路由协议的收敛等提供良好的基础，因此逻辑设计阶段，对于网络层地址的分配应遵循一些特定的原则。

1．使用结构化网络层编址模型

网络层地址的结构化模型是对地址进行层次化的规划，例如 IP 协议的地址本身就是层次化的，分为网络前缀和主机两个部分。使用结构化网络层编制模型的基本思路是首先为企业网络分配一个 IP 网络号段，然后将网络号分成多个子网，最后将子网划分成为更细的子网。

采用结构化网络层编址模型，有利于地址的管理和故障排除。结构化使得理解网络结构、网管软件实施管理、协议分析设备的分析和报告生成都相对较为容易，同时由于结构化网络地址在路由器、防火墙等设备上的过滤规则表达的优势，也使得网络优化和网络安全易于实现。

2．通过中心授权机构管理地址

一个企业的信息管理部门应该为网络层编址提供一个全局模型，而网络设计者必须先提供这个参考模型，这个模型应该根据核心、汇聚、接入的层次化，对企业各个区域、分支机构等在模型中的位置进行明确标识。

在企业网络中，IP 地址由两类地址构成，分别为公有地址和私有地址。私有地址多是一些保留地址段，只在企业网络内部使用，企业信息管理部门拥有对地址的管理权。公有地址是全局唯一的地址，并且必须在授权机构注册才能使用。

在设计阶段，必须明确如下内容：

- 是否需要公有地址和私有地址。
- 只需要访问专用网络的主机分布。
- 需要访问公网的主机分布。
- 私有地址和公有地址如何翻译。
- 私有地址和公有地址的边界。

3．编址的分布授权

与编制模型匹配的是一个地址授权管理中心以及相应的管理制度，该中心不仅可以直接管理网络地址，还可以根据需要在网络区域、分支结构内建设分中心，授权分中心的管理人员对区域的地址进行管理。

在各分支机构管理人员网络管理业务较强、网络规模较大的情况，可以采用分布授

权模式，由设计人员依据结构化模型，将各个地址段的编址和管理分配于相应的分支机构。

如果分支机构的管理人员缺乏经验，则不能采用分布授权方式，而采用集中管理方式，以避免误操作以及网络失效带来的故障。

4．为终端系统使用动态编址

对于频繁变更位置、移动性较大的终端用户，采用静态的网络地址不利于管理，动态编址协议的使用既可以保证分配的地址纳入管理范畴，又可以减少管理工作量。

在 TCP/IP 体系中，主要使用 DHCP 来完成终端主机的 IP 地址和域名自动获取。

DHCP 使用客户机/服务器模型，服务器分配网络地址，并保存已分配地址信息；客户机从服务器动态请求配置参数。DHCP 支持三种 IP 地址分配方法。

- 自动分配：服务器为客户机分配一个永久的 IP 地址。
- 动态分配：服务器在一个有限的时间段内，为客户机分配一个 IP 地址，在使用完毕后予以回收。
- 手工分配：由网络管理员为客户机分配一个永久 IP 地址，DHCP 仅用于将手工分配的地址传送给客户机。

动态分配是较为流行的方法，通过租用机制，可以保证有限的地址为大量的不同时段的客户机提供地址分配服务，并且动态分配地址减少了管理人员的工作量。

设计人员在逻辑设计阶段必须确定如下问题：

- 可以使用自动分配的客户机群落。
- 可以使用动态分配的客户机群落。
- DHCP 可以管理的 IP 地址段。
- DHCP 的逻辑网段位置等。

5．私有地址的使用

私有地址可以用于企业内部的地址，这些地址相互之间可以访问，但是在访问公网地址时，必须进行转换。

在 RFC1918 中，IETF 为内部使用的私有地址预留了如下的地址段：

- 10.0.0.1～10.255.255.255
- 172.16.0.0～172.31.255.255
- 192.168.0.0～192.168.255.255

私有地址的存在使得网络内部安全性提高，外部网络无法发起针对私有网络地址的攻击；私有地址不需要授权机构的管理，灵活性强；私有地址可以避免大量公有地址的浪费。但同时，也具备一些缺点，如网络管理一旦外包，则很难实施管理；地址分配容易造成混乱的情况；另外，由于大多数用户使用的私有地址段都是相近的，在实现 VPN 互联时，很容易造成地址冲突。

设计人员必须设计出私有地址与公有地址的转换方式，目前在地址转换方面主要有

三种技术，分别是 NAT、PAT 和 Proxy。

NAT 技术是由网络管理员提供一个公有 IP 地址池，私有地址的主机在访问公有网络时，建立起私有地址和地址池中某一个 IP 地址的映射关系，从而访问公有网络。

PAT 技术是多个私有地址共用一个公有 IP 地址，在两种地址的边界设备上，建立起端口的映射表，这个表主要由私有源地址、私有地址源端口、公有地址源端口组成，通过这种映射关系来完成多个私有地址访同时访问公有网络。

Proxy 不是工作在网络层的地址转换技术，主要是工作在应用层，由代理软件完成数据包的地址转换工作。

2.5.6.2 使用层次化模型分配地址

层次化编址是一种对地址进行结构化设计的模型，使得地址的左半部分的号码可以体现大块的网络或节点群，而右半部分可以体现单个网络或节点。层次化编址的主要优点在于可以实现层次化的路由选择，利于在网络互联路由设备之间分发网络拓扑结构。

1．层次化编址的优势

在编址和路由选择模型中使用层次化模型具有如下好处：

- 易于排查故障。
- 易于管理和性能优化。
- 加快路由选择协议收敛。
- 需要更少的网络资源。
- 可扩展和稳定性强。

层次化编制允许对网络号进行汇总，这使得路由器在通告路由表时对路由规则条目相应进行汇总；另外该编址方式易于实现可变长度子网掩码（VLSM），为子网的划分添加了灵活度，优化可用地址空间。

2．层次化路由选择

层次化路由的含义是指对网络拓扑结构和配置的了解是局部的，一台路由器不需要知道所有的路由信息，只需要了解其管辖的路由信息，层次化路由选择需要配合层次化的地址编码。

设计人员在进行地址分配时，为配合实现层次化的路由器，必须遵守一条简单的规则——如果网络中存在着分支管理，而且一台路由器负责连接上级机构和下级机构，则分配给这些下级机构网段的地址应属于一个连续的地址空间，并且这些连续空间可以用一个子网或者超网段表示。例如一台路由器上连总部，下连 4 个分支机构，每个分支机构都分配一个 C 类地址段，整个企业网络申请的地址空间为 202.103.64.0 — 202.103.79.255 （202.103.64.0/20 ）；则对这 4 个分支机构应该分配连续的 C 类地址，例如从 202.103.64.0/24～202.103.67.0/24，这 4 个 C 类地址可以用 202.103.64.0/22 这个超网来表示。

3．无类路由选择协议

IP 地址分为两个部分，分别为网络号和主机号，IP 地址本身被分为多种类型，分别为 A，B，C 类地址。传统的路由协议只识别分类地址，也就是说路由表项是以类型地址为依据而产生，这种路由协议被称为分类路由选择协议。

采用这种传统方式，不仅仅会导致大量的地址浪费，而且会导致路由表项数量过多；为避免 IP 地址的浪费，开始出现了子网的概念以及可变长度子网掩码概念，这使得网络的表示方式发生了很大的变革，典型的对网络的表示方法就是使用长度字段来表示前缀的长度，例如地址 10.1.0.1/16，表示这是一个地址范围为 10.1.0.0～10.1.255.255 网络（可以用 10.1.0.0/16 表示）中的主机地址，其主机部分为 0.0.0.1。基于这些变革，产生了无类路由选择协议，这些协议不基于地址类型，而是基于 IP 地址的前缀长度，允许将一个网络组作为一个路由表项，并使用前缀说明哪些网络被分在这个组内；确切地说，无类路由选择协议支持任意的前缀长度。

设计人员在进行选择时，应尽量采用无类路由选择协议，包括 RIP V2、OSPF、GBP、IS-IS 等。

4．路由汇聚

无类路由选择协议通过路由和前缀长度，如果地址是层次化方式分配的，则无类路由选择协议可以将多个子网或网络汇聚成一条路由，从而减少路由选择协议的开销，这种汇聚工作的重要性，在企业网络设计中同样重要，因为路由汇聚意味着一个区域的问题不会扩散到其他区域。

在进行 IP 地址规划时，为了保证各个层次路由汇聚的正确性，需要根据 IP 地址的分配情况，对路由汇聚进行验证，可针对分配方案和地址预留方案，依据下列规则对各个路由器的下联网络进行路由汇聚测试，以便于及时找到扩展性等方面的问题。

- 可以汇聚的多个网络 IP 地址的最左边的二进制必须相同。
- 路由器必须依据 32 位的 IP 地址和最长可达 32 位长的前缀长度确定路由选择。
- 路由协议必须承载 32 位地址的前缀长度。

5．可变长度子网掩码

使用无类路由选择协议，意味着在单一网络中可以有大小不同的子网，子网大小的变化就是通常所说的可变长度子网掩码（VLSM）。VLSM 依据显示提供的前缀长度信息使用地址，在不同的地方可以具有不同的前缀长度提供了实用 IP 地址空间的效率和灵活性。

因此，设计人员只要准备采用无类路由选择协议，就可以在网络内部根据需要任意划分不同规模的网段，并采用可变长度子网进行表示。

2.5.6.3 设计命名模型

命名在满足客户易用性目标方面起到了非常关键的作用，简短而有意义的名字可以

帮助用户非常简洁地定位服务的位置；设计人员应该从资源的角度设计出易用性、可管理性强的命名模型，以便于提高网络用户的体验度。

在企业网络中，需要进行命名的资源较多，包括路由器、交换机、服务器、主机、打印机以及其他资源，借助于优秀的命名模型，网络用户可以直接通过便于记忆的名字而不是地址透明地访问服务器。

在网络命名系统中，将名字映射到地址的方法主要包括两种类型，一种是使用命名协议的动态方法，一种是借助于文件等方式的静态方法。

网络中的命名主要涉及 NetBIOS 名字和域名两个方面。

1. 命名的分布授权

企业网络的命名管理需要建设一个特定的中心授权机构以及相应的管理制度，命名的授权管理可以采用集中方式，也可以采用分布授权方式。由于名称管理的特殊性，命名自身的层次性，并且名称将直接面对客户，大多数情况下都采用分布授权，这样可以提高分支机构对自身内部名称变更的快速性。

2. 分配名字的原则

在对网络资源进行命名，并分配具体名称时，需要遵循一些特定的原则：

- 增强易用性，名字应该简短、有意义、无歧义，用户可以很容易地通过名称来对应各类资源，例如交换机使用 sw 作为开头、服务器使用 srv、路由器使用 rt 等。
- 名字可以包含位置代码，设计人员可以在名字模型中加入特定的物理位置代码，例如第几分公司、总部等特殊的代码。
- 名字中应尽量避免使用连字符、下划线、空格等不常用字符。
- 名字不应该区分大小写，否则会导致用户使用的不方便。

3. NetBIOS 名字

NetBIOS 是一个具有设备命名功能的应用编程接口，而 NetBIOS 名字是网络中应用进程的唯一名称。NetBIOS 名字为微软 Windows 平台的客户机和服务器之间的应用访问、文件共享提供了编址基础。

NetBIOS 具备自己独立的名字解析概念和能力；在 NetBIOS 中，计算机需要首先注册自己的名字，才能解析该名字。从 NetBIOS 名字查找相应的节点地址（TCP/IP 协议中为 IP 地址）有几种不同的查找方式。

- 本地广播：广播自己的 NetBIOS 名字，完成注册和查询对应 IP 地址的工作。
- 缓冲：支持 NetBIOS 的计算机都维护 NetBIOS 名字和 IP 地址的临时列表。
- 名字服务器：通过 WINS 服务器实现 NBNS（NetBIOS Name Server）功能，计算机通过 NBNS 完成注册与查询工作。
- Lmhosts 文件：本地文件 lmhosts 存放着手工设定的 NetBIOS 与 IP 的对应关系，以便于计算机查询。
- DNS/hosts 方式：在其他方法都无法查询时，可以借助于 DNS 和 hosts 文件实现

名字与 IP 的转换。

网络设计人员需要在这些不同的查找方式中进行选择，确保局域网络具有正常的 NetBIOS 注册和解析能力。

4．域名解析

DNS 用于完成难于记忆的 IP 地址与域名之间的转换，主要有两项功能，分别为正向解析（forward domain）与逆向解析（reverse domain）。正向解析的主要任务是将域名转换为数字的 IP 地址，以便网络应用程序能够正确地找到需要连接的目标主机；逆向解析的主要任务是将数字的 IP 地址转换为域名。

DNS 并不像简单的客户机/服务器系统，仅仅由客户机提出请求，而 DNS 服务器给出应答，单凭一台 DNS 服务器无法完成庞大而复杂的域名解析工作，解析工作由无数 DNS 服务器所构成的分步式系统所共同完成，如图 2-67 所示。

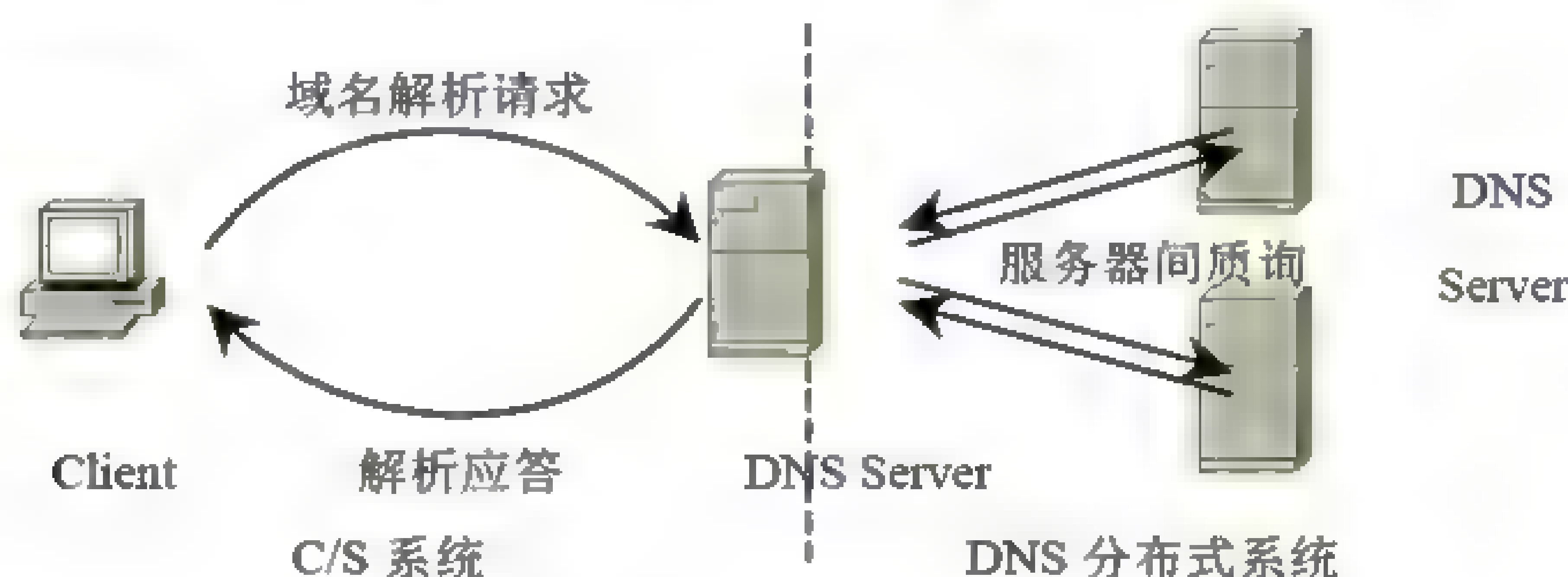


图 2-67　DNS 系统

DNS 的域名服务器进程按功能可以分为 4 类，分别为主服务器（Primary/Master DNS Server）、次服务器（Secondry/Slave DNS Server）、缓存服务器（Cache）和解析服务器（Resolver）。主服务器负责维护某个域的域名解析数据库，并向其他主机提供域名查询；次服务器利用区域传送，从主服务器复制网络区域内的域名解析数据，当主服务器不能正常工作时，次服务器就可以向外界提供查询；缓存服务器的功能是缓存域名解析的结果，减轻域名服务器的负荷；解析服务器是一个客户端软件，执行本机的域名查询。每台 DNS 服务器主机上都由二种或三种服务器进程共同提供 DNS 服务。

另外 DNS 中没有专门的逆向解析，逆向解析是借助于一个特殊域（in-addr.arpa）的正向解析来完成的。

设计人员应该确定网络系统中的 DNS 服务器数量和类型，同时对需要进行正向解析的域名区域、逆向解析的 IP 地址范围进行确定。

2.5.7　路由选择协议

路由选择协议使路由器能够自动学习如何达到网络，并与其他路由器交换路由信息，以达到全网路由选择的目的。路由选择协议的选择是网络设计中的重要内容，直接

决定了网络的连通性、稳定性。

2.5.7.1 路由协议选择原则

1．路由协议类型选择

路由选择协议分为两大类：距离向量协议和链路状态协议，这两种协议的特征在前述章节已经进行了介绍。网络设计人员可以依据以下的条件在两种类型中进行选择。

当满足下列条件时，可以选择使用距离向量路由选择协议：

- 网络使用一种简单的、扁平的结构，不需要层次化设计。
- 网络使用的是简单的中心辐射状结构。
- 管理人员缺乏对路由协议的了解，路由操作能力差。
- 收敛时间对网络的影响较小。

当满足下列条件时，可以选择使用链路状态路由选择协议：

- 网络采用层次化设计，尤其是大型网络。
- 管理员对链路状态路由协议理解较深。
- 快速收敛对网络的影响较大。

2．路由选择协议度量

当网络中存在多条路径时，路由协议使用度量值来决定使用哪条路径。不同的路由选择协议的度量值是不同的，传统协议以路由器的跳数作为度量值，新一代的协议还将参考延迟、带宽、可靠性及其他因素。

对度量值存在着两个方面的考虑：一是对度量值的限制设定，例如如果设定基于跳数路由协议的有效路径度量值必须小于16，这些度量值的设定直接决定了网络的连通性和效率；二是多个路由协议共存时的度量值转换，路由器上可能会运行多个协议，不同的路由协议对路径的度量值不同，设计人员需要建立起不同度量值之间的映射关系，让多个协议之间相互补充。

3．路由选择协议顺序

路由器上可能会存在多个不同的路由协议，针对一个目标网络，这些路由协议都会选举出具有最小度量值的路径，但是不同协议的度量值不同，可比较性较小。设计人员建立的协议度量值的转换关系只是用于不同路由协议之间的路由补充，不能用于具体路径的选择。

因此，设计人员可以在网络中运行多个路由选择协议，并约定这些协议之间的顺序，这些顺序可以用路由协议权值来表示，权值最小的协议顺序越靠前；一旦多个路由协议都选举出了最优路径，则具有最小权值的路由协议的路径生效。

4．层次化与非层次化路由选择协议

路由协议从层次化角度可以分为支持和不支持两种；在非层次化协议中，所有路由

器的角色都是一样的；层次化协议中，不同路由器的角色不同，需要处理的路由信息量也不同。

对于采用层次化设计的网络来说，最好采用层次化路由选择协议。

5．内部与外部路由选择协议

路由协议根据自治区域的划分以及作用，可以分为内部网关协议和外部网关协议，设计人员需要选择正确的、合适的协议类型；例如对于内部网关协议，较为常见的是 RIP、OSPF、IGRP，对于外部网关协议，多选择 BGP 协议。

6．分类与无类路由选择协议

分类与无类路由协议的选择在前文中已经进行了介绍，是进行网络路由设计时必须考虑的内容。

7．静态路由选择协议

静态路由指手工配置并且不依赖于路由选择协议进行更新的路由，静态路由经常用于连接一个末梢网络，也就是指只能通过一条路径到达的网络部分，静态路由的最常见的使用方法就是默认路由。网络设计人员应该对设计网络中的末梢网络进行区分，并设定这些末梢网络的默认路由。

静态路由一般情况下要比其他动态路由协议级别高，也就是说即使通过动态路由协议选举出一条最优路径，数据包仍然会依据静态路由制定的路径进行传递，因此设计人员需要根据实际需要来确定静态路由选择协议的范围，以免使得动态路由协议失效。

最后，静态路由信息可以导入到动态路由选择协议形成的路由表项中，形成路由信息的互补关系。

2.5.7.2　内部网关协议——OSPF

OSPF 协议是典型的、应用最广的内部网关协议，该协议为层次化、无类路由选择协议，在前文中已经对 OSPF 的相关概念进行了介绍，以下是 OSPF 协议的一些常见应用规则，在实际应用中可根据需要进行调整。

1．OSPF Router ID

原则上采用网络设备的 loopback 0 或 loopback 1（考虑到某些厂商设备在不支持 loopback 0 时采用 loopback 1）的接口地址作为设备的 Router ID。Router ID 应统一规划，作为路由域内该设备的唯一地址标识以及管理地址。

2．OSPF 时间参数

- Hello 包间隔时间为 1s。
- 相邻路由器间失效时间为 3s。
- LSA 更新报文时间为 1s。
- 邻接路由器重传 LSA 的间隔为 5s。
- OSPF 的 SPF 计算间隔为 5s。

- 外部路由引入采用 OE1 方式（即到外部路由的花费值=本路由器到相应的 ASBR 的花费值+ASBR 到该路由目的地址的花费值），原则上只引入需要发布的路由；域间路由条目的发布只发布域汇总路由信息（路由条目≤4 条）。
- 采用 MD5 对报文（接口、区域）验证。

3．OSPF COST

COST 为 OSPF 协议的度量值，可以根据连接的带宽设定不同链路的 COST 值，表 2-16 是对常见链路带宽的 COST 值设定，可根据设计人员的工程经验进行调整。

表 2-16 常见带宽链路 COST 值设定

带宽或链路	COST 值
10Gbps 或 SDH STM-64	1
2.5Gbps 或 SDH STM-16	3
1Gbps	8
155Mbps 或 STM-1	50
100Mbps	80
10Mbps	800
4*E1	1000
E1	4000

4．OSPF DR 与 BDR

OSPF DR 与 BDR 选择应遵循以下规则：

- 应手动指定，上级设备为 DR。
- OSPF 接口上所有网络类型均配置为广播。
- OSPF 区域支持报文验证。
- ABR 与 ASBR 应自顶向下通过第 5 类 LSA 发布默认路由。
- 在核心路由器上建议配置 OSPF 路由过滤，包含对引入和发布的路由都需要过滤（推荐配置策略只允许合法路由条目发布和接受）。
- 禁止 loopback 接口发送 OSPF 报文。
- 禁止采用 OSPF 虚连接的方式连接区域。

2.5.7.3 外部网关协议——BGP

BGP 是典型的外部网关协议，也是应用最广的外部网关协议，在前文中已经对 BGP 的相关概念进行了介绍，以下是 BGP 协议的一些常见应用规则，在实际应用中可根据需要进行调整。

1．BGP 对等体

- 对不同对等体组应定义易于记忆、无歧义的组名。

- 建议不要将 IBGP 对等体和 EBGP 对等体加入同一个组中。
- 不允许同不直接相连网络上的 EBGP 对等体（组）建立连接。

2．BGP 时间参数

- BGP Keepalive 报文的发送时间间隔为 5s。
- 保持定时器为 15s。
- IBGP 对等体（组）发送路由更新报文的时间间隔为 1s。
- EBGP 对等体（组）发送路由更新报文的时间间隔企业网内部为 5s，企业网外部为 30s。

3．BGP 本地优先级

BGP 要求配置本地优先级属性，本地优先级的值为 100。

4．BGP MED

由多个 AS 构成的层次模型中，下级 AS 到上级互连 MED 值为 1，同级间 AS 互连 MED 值为 0（MED 值小的优先级高）。

5．BGP 联盟

一个 IBGP 域内只能存在一个联盟并且联盟 ID 号与 AS 号保持一致。

6．BGP 同步

建议关闭 BGP 与 IGP 的同步。

7．BGP 路由发布

只在做 MPLS-VPN 时 BGP 与 IGP 进行交互，原则上只允许在 PE 设备上交互。

8．BGP 路由过滤

在 BGP 接受路由信息时需要做基于 IP 前缀的路由过滤。

9．静态路由

为避免路由环路的生成，对已部署动态路由的连接关系，不允许在动态路由部署的连接关系上重复部署静态路由。

2.5.8　网络管理

网络管理并不是单纯的技术工作，而是行政管理工作与技术管理共同组成的复杂体。在目前网络管理技术快速发展的同时，行政管理明显出现了滞后的现象；导致网络运行故障的原因很大一部分并不是来自于网络管理技术上的漏洞，而是来自于行政管理上的疏忽或错误。

在进行网络设计时，为加强网络管理工作的有效性，应将网络的管理手段分为两大类，分别是行政管理和技术管理，其中技术管理又依据管理技术的层次性划分为 TMS（传输管理系统）、NMS（网络管理系统）、RMS（资源管理系统）和 AMS（应用管理系统）。网络管理手段的构成情况如图 2-68 所示。



图 2-68 网络管理手段构成

2.5.8.1 行政管理手段

通常情况下网络管理中心是企业网络管理、维护的核心部门，在网络管理中心设计和建立完善的行政管理制度是保证网络平台稳定运行的关键。

1．机构设置

典型的网络管理中心由办公室、网络运行室（NOC）、网络信息室（NIC）三个机构构成，设立网络中心主任、副主任、秘书、网络管理员、网络信息员等多个岗位，其常见的机构组成情况如图 2-69 所示，设计人员可以参照形成不同网络平台的网管中心组织结构。

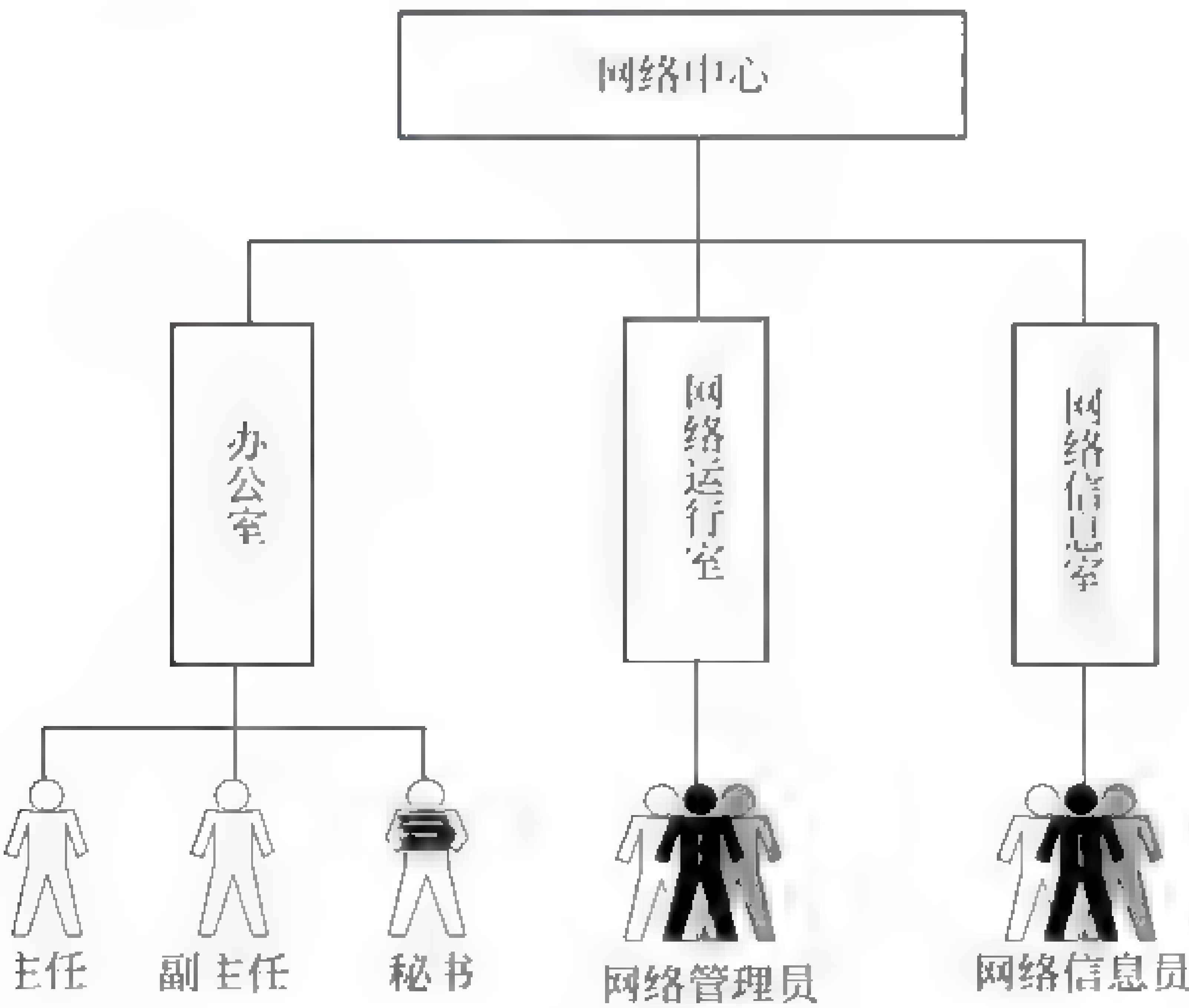


图 2-69 网络管理中心常见组织机构

2．岗位职责

设计人员在进行主要岗位职责设计时，可以参照以下内容进行岗位职责设计。

（1）主任职责：负责处理信息网络中心重大事项。

- 组织编制网络信息化建设规划。
- 审核、批准网管中心的日常开支。
- 批阅上级来文，交相关人员处理。
- 负责信息网管中心的人事与工作安排。
- 协调与有关领导、有关职能部门的关系。
- 完成领导交办的其他工作。

（2）副主任职责：主持网管中心的日常工作，协助主任处理信息网络中心的重大事项。

- 主持网管中心业务发展工作。
- 编制年度的信息建设发展规划。
- 编制年度的网络建设计划。
- 制订有关信息和网络方面的重要规章制度、管理规范和信息标准。
- 主持制订信息建设项目的规划、建设和管理。
- 主持企业网络重要建设项目的规划、设计、建设和管理。
- 根据有关规定和网管中心的需要，拟订有关的招标、评标文件。
- 对外联系与内部协调。

（3）网络管理员职责：负责网络平台的系统管理与维护，确保网络安全、高效、稳定地运行。

- 网络基础设施管理，包括负责网络主干设备的安装与维护，掌握网络主干设备的配置情况及配置参数变更情况，及时备份各个设备的配置文件等。
- 系统监控，包括了解和记录与外部网络的连通情况，实时监控整个网络平台的运行和网络通信流量情况；对出现的问题及时汇报并采取相关措施解决等。
- 网络设备的端口管理，包括了解和记录用户设备接入网络的情况，对发现的问题及时定位和处理，及时更新用户变更数据等。
- 网络服务器管理，包括安装和管理所需的网络操作系统，管理和维护 DNS、E-mail、数据库等相关服务器，随时了解和记录系统配置情况及配置参数变更情况，并对配置参数进行备份等。
- 网络安全管理，包括网络安全与保密软硬件管理，采取各种有效措施防止病毒、非授权用户的入侵和设备配置密码的泄露，及时更新操作系统的补丁，封堵各种网络设备配置的漏洞等。
- IP 地址资源的分配与管理，形成完整的维护文档。
- 设备资料的管理工作。
- 网络分担交费与查询工作。

（4）网络信息员职责：负责企业内外门户的建设与维护，面向各类用户提供信息服务、信息处理与统计等。

- 负责企业内外门户的信息更新。
- 负责门户网站的设计、建设与维护。
- 开发和建设公共服务信息管理系统，提供公共服务信息的发布、查询等功能。
- 相关系统数据的备份与恢复。
- 面向企业各行政部门提供 Web 服务器空间租用、虚拟主机、服务器托管等信息服务工作。
- 电子邮件账号管理，提供包括开户、修改、暂停、注销等服务。
- 企业网络用户管理。

3. 管理制度

为配合网管中心工作人员实施网络管理，同时通过制度化保证管理的力度与效果，网络管理中心还必须制定各项管理制度，其主要内容包括：

- 《网络管理中心值班制度》
- 《网络管理中心出入人员管理制度》
- 《网络管理中心密码管理制度》
- 《网络管理中心安防制度》
- 《网络管理中心设备管理制度》
- 《网络管理中心用户管理制度》
- 《网络管理中心设备配置与维护制度》
- 《网络管理中心服务器配置与维护制度》
- 《网络管理中心故障申报与处理制度》
- 《网络管理中心操作规范》
- 《网络管理中心工作考核制度》
- 《网络管理中心技术考核制度》
- 《网络管理中心紧急事故处理预案》

2.5.8.2 传输管理系统

传输管理系统（TMS）是网络平台传输线路管理的主要管理工具，随着网络规模的发展，连接的远程分支也逐步增多，在一个大型网络中，大量的传输线路构成了网络的基础，而 TMS 就是对这些传输线路进行管理的系统，这些系统含有对光纤资源、SDH 电路等物理或逻辑线路状态、参数等的实时管理与监控。

传输管理系统必须借助于专业的信令网络，并且投资较大，作为企业网管中心这样的非营利性机构，是无法建设如此规模的传输管理系统的；常见的建设方式是由网络平台的线路提供商向企业网络管理中心提供 TMS 管理终端或者相应的开发包，集成商技术人员在此基础上形成相应的定制管理终端，由企业网络管理人员在终端上实施管理。

2.5.8.3　网络管理系统

网络管理系统（NMS）是较为经典的网络管理方式，在 ISO 组织规定的网络管理基本功能中，网络管理功能被划分为配置管理、安全管理、故障管理、费用管理和性能管理五大部分；目前基于网管协议 SNMP-Ⅰ、SNMP-Ⅱ和 SNMP-Ⅲ的网络管理产品已经十分成熟，已经涌现出 HP 的 OpenView、Sun 的 SNM、IBM 的 NetView、Cisco 的 CiscoWorks 等应用较广的网络管理产品。

设计人员应根据网络管理员的需求进行 NMS 产品的设计，大多数网络平台对网络管理系统产品都有如下的功能需求：

（1）能自动发现网络拓扑结构的变化。

（2）能够自动搜索网络设备，并根据搜索结果分析网络结构。

（3）能够管理多种网络设备，能够管理异构网络。

（4）至少支持 SNMP-Ⅰ、SNMP-Ⅱ、SNMP-Ⅲ管理协议。

（5）具有图形化操作界面，交互性好。

（6）可以定义定时器，定期查询网络设备的 MIB 对象。

（7）可以定义基于 MIB 对象的事件，在 MIB 对象的参数值达到一定阈值后触发事件发生，并以多种形式通知网络管理员（电子邮件、声音提示、屏幕闪烁）。

（8）采用分布式设计，网络平台中可以存在多个管理工作站，并且这些工作站之间具有管理上的层次性。

（9）可支持将 MIB、日志、审计等数据以多种形式存放，例如文本文件、多种网络数据库产品等。

（10）在 Windows、UNIX 等多种操作系统中都有相应的产品系列。

（11）支持 B/S 的网络管理方式。

2.5.8.4　资源管理系统

综合资源管理就是要建立一个完整的网络视图，包括传输网络、信令网络和数据网络，同时能体现各个网络之间的关联关系；系统能管理网络资源和地理信息之间的关联关系，操作人员很方便地了解网络资源在地理上的分布情况；还包括机房、管线等非智能的设备等的视图。

在网络层次中，网络资源管理系统处于整个网络运营管理支撑系统的基础和核心，其主要功能包括网络规划、网络设计、网络资料管理、网络资源调度、工程施工、网络维护、网络质量管理。

网络资源管理系统将成为业务管理系统运作的基础，将给业务管理系统（业务管理层）提供调用接口，主要是资源分配使用（调度）和资源查询，业务管理系统将根据资源配备情况进行任务分配。

图 2-70 是一个典型的网络资源管理系统的设计构成图，设计人员可参照形成不同网络工程的资源管理系统。

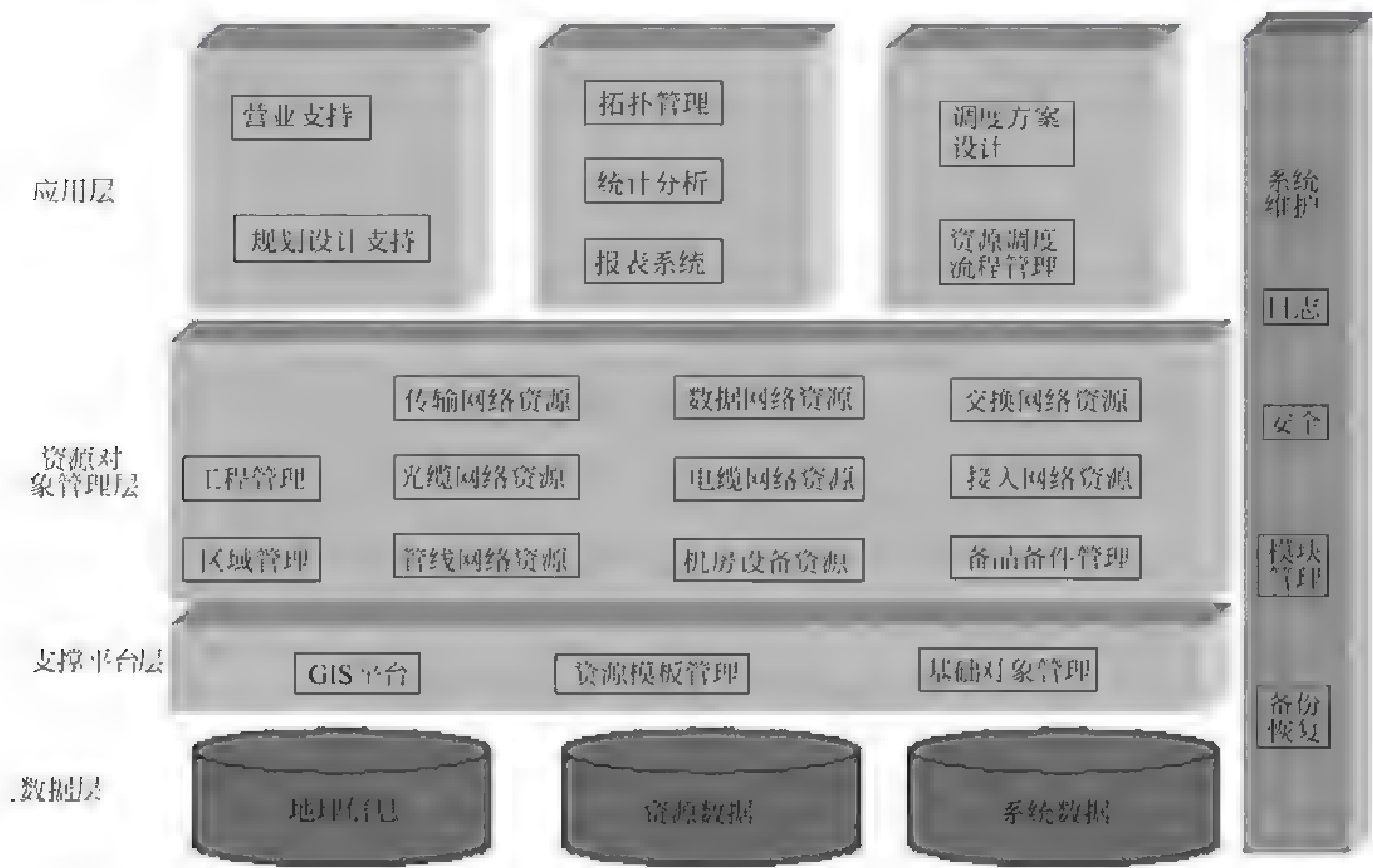


图 2-70 网络资源管理系统构成

- 数据层：基于共享数据模型进行网络资源的数据模型定义，并针对集中数据库和分布式数据库要求完成数据库的逻辑和物理设计。
- 支撑平台层：网络资源管理中一些基本的操作元素和功能模块，包括基础对象管理、模板管理、GIS 平台、动态查询定制管理等。
- 资源对象管理层：支持话务网、传输网、信令网、支撑网、同步网、智能网、空间资源、短消息、客服中心等电信全部网络资源对象的管理，并支持各专业网络资源的关联管理。
- 应用层：支持具体业务操作的组件，包括网络效率评估、资源调度调配、资源预警分析等。

在采用成熟产品实现网络资源管理时，所采用的产品必须具备以下功能：

- 跨平台运行。
- 提供实时的消息通信机制。
- DataCache 技术保证资源的快速访问。
- 集中管理，分布应用实现资源的集中管理。

- 多角度的资源组织视图提供资源显示形式。
- 任意资源定位、故障定位技术，保证资源的快速查询和定位。
- 提供丰富的与上层资源应用的接口。

2.5.8.5　应用管理系统

应用管理系统（AMS）目前的概念较为模糊，与资源管理系统有一定的重合，但是AMS 更加注重对用户服务的管理，通过对运行于服务器上的用户服务进程实施监视，来实现对应用资源的管理。

大多数企业网络的应用管理系统必须采用专有设计，应用管理系统的主要监控对象是两部分内容：一部分是向网络用户提供的各种 Internet、Intranet 上的服务，例如 WWW、FTP、Telnet、SMTP 等；一部分是网络平台上运行的各类专业应用系统，例如财务系统、OA 系统、生产系统、销售系统等。在设计方面，应用管理系统应该采用多个服务状态采集器、一个中心管理工作站的分布方式，如图 2-71 所示。

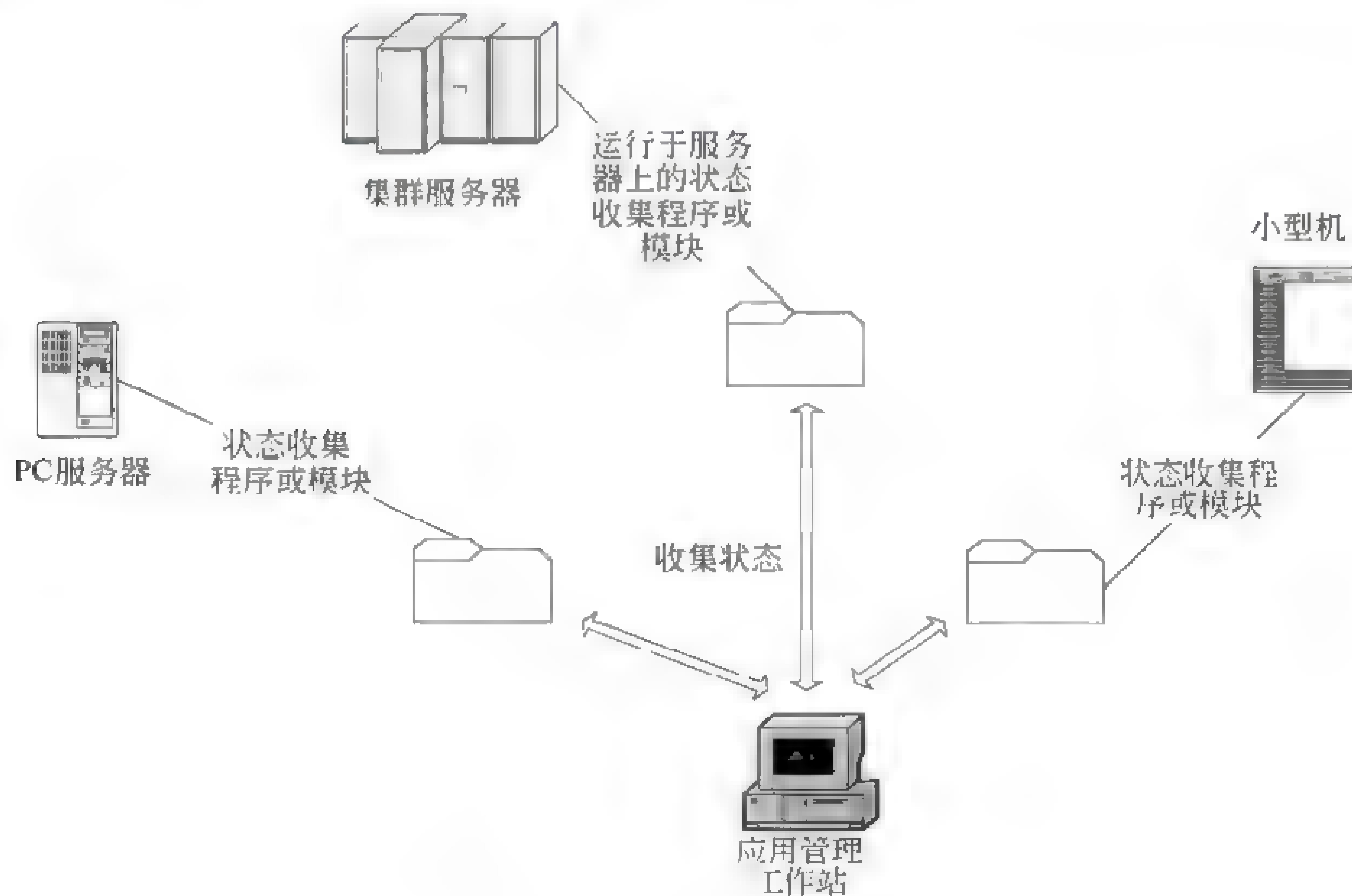


图 2-71　应用管理系统示意图

在设计应用管理系统时，由于企业网络中运行的服务除 Internet、Intranet 上的通用服务之外，大多数都是专用业务系统，所以必须制定应用管理协议，并以协议为基础针对各种通用服务器和专用服务分别开发出应用服务状态收集程序或模块；这些程序运行于服务器上，不断收集服务进程的状态，并通过网络提交给应用管理工作站；应用管理

工作站在收到状态报告后，根据状态异常统计、模式匹配等方法发现应用系统的非正常状态；在发现服务处于非正常状态后，通过短信、报警等多种方式通知管理员。

2.5.9 网络安全

网络安全体系设计是逻辑设计工作的重要内容之一，在设计网络体系时存在多种安全架构模型，本章节将依据图 2-72 的安全架构模型进行网络安全体系设计的介绍。

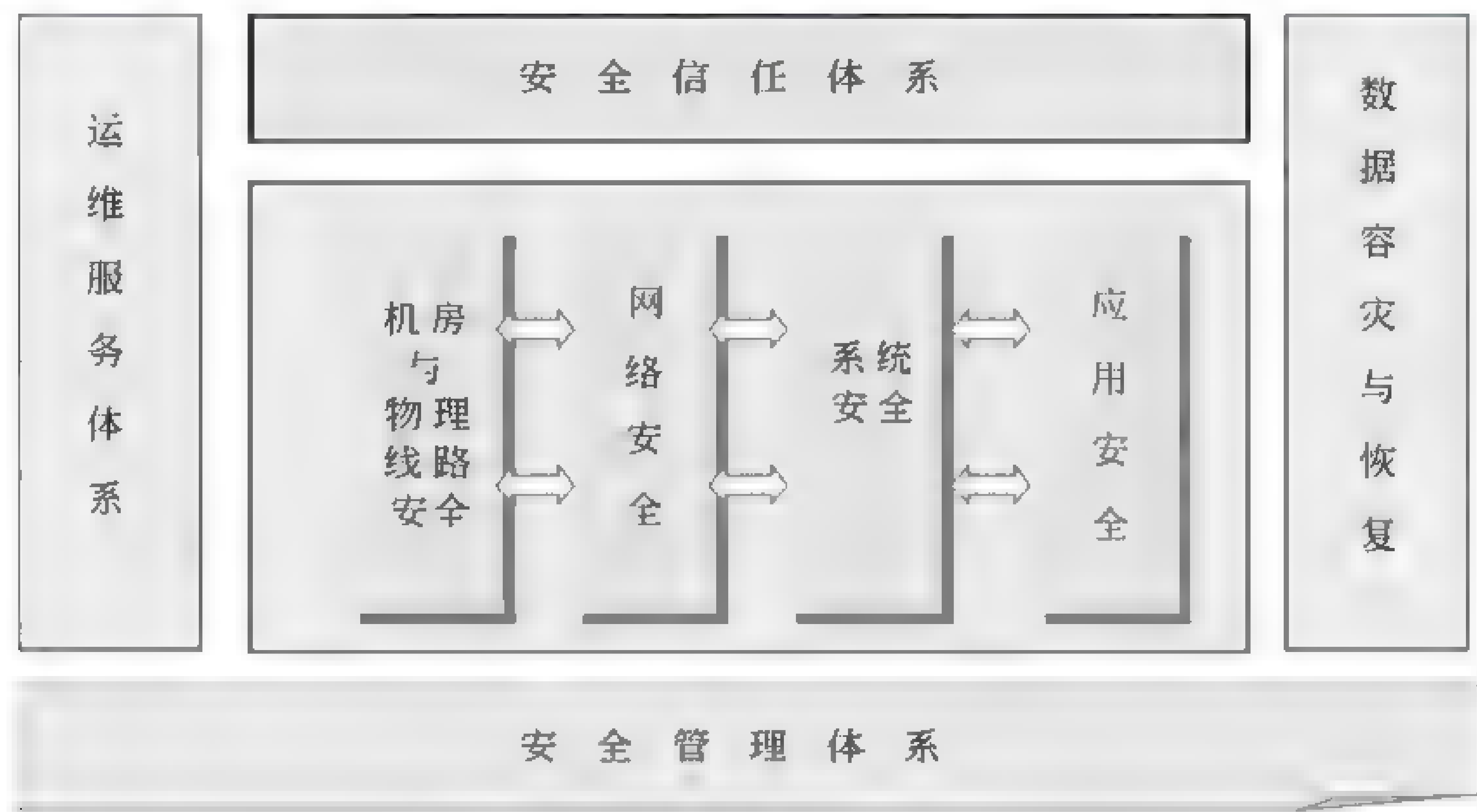


图 2-72 安全体系总体安全架构

该安全体系的特点如下：

- 以人为本的安全管理体系是整个安全架构的基础，使安全问题可控可管。
- 以安全技术为核心的技术措施（包括机房及物理线路安全、网络安全、系统安全、应用安全、安全信任体系等），使安全手段更加可靠。
- 以容灾与恢复为目标的后备保障措施，可以对付重大灾难性事件后的网络重建。
- 以安全运维支持服务作为外部支撑条件，使安全问题能够及时有效地解决。

2.5.9.1 机房及物理线路安全

机房及物理线路安全主要是指存放、支撑网络设备运行的物理环境设施及物理线路情况。

1. 机房安全

机房、UPS 电源、监控等场地设施和周围环境及消防安全，应符合国家相关标准，并满足网络平台运行的要求，例如 7×24 小时运行或 5×8 小时运行。

机房的安全措施应符合 GB/T 9361—1988、GB/T 2887—1989 的要求。

2．物理线路安全

1）计算机通信线路安全

计算机通信线路是实现数据传输的物理线路，包括网线、光纤等。应符合以下要求：

- 通信线路采用铺设或租用专线方式建设。
- 通信线路应远离强电磁场辐射源，埋于地下或采用金属套管。
- 定期测试信号强度，以确定是否有非法装置接入线路；特别是在线路附近有新的网络架设、电磁企业开工时，应该请专业机构负责检测。
- 定期检查接线盒及其他易被人接近的线路部位，防止非法接入或干扰。

2）骨干线路冗余防护

骨干线路冗余防护应符合以下要求：

- 骨干线路或重要的节点与网络平台相连，应有冗余线路和环形路由措施。
- 骨干线路的网络设备应有冗余电源配置，保障线路正常运转。
- 重要部门重要业务系统所属的相关线路，应建立冗余或环形路由措施。
- 大型网络的互联网出口线路应建立冗余线路并以负载均衡的方式运行。

3）骨干线路和主要设备的防雷击措施

计算机通信线路骨干线路和核心设备，应该具备防雷击的措施。

2.5.9.2　网络安全

1．安全域划分

网络平台安全域通常可以划分为：核心局域网安全域、部门网络安全域、分支机构网络安全域、异地备灾中心安全域、互联网门户网站安全域、通信线路运营商广域网安全域等，另外，核心局域网安全域又可以划分为中心服务器子区、数据存储子区、托管服务器子区、核心网络设备子区、线路设备子区等多个子区域；在实际的网络工程中，设计人员可根据需要自行进行安全域的划分。

2．边界安全策略

1）边界安全总体策略

网络的边界安全访问总体策略为：允许高安全级别的安全域访问低级别的安全域，限制低级别的安全域访问高安全级别的安全域，不同安全域内部分区进行安全防护，做到安全可控。

下列设计规则将依据常见的安全区域方法，对主要的边界规则进行介绍。

2）核心网络与互联网的边界

核心网络与互联网的边界的安全措施设计应符合以下要求：

- 应部署逻辑隔离措施，主要是防火墙隔离。
- 允许互联网用户访问网络 DMZ 区域的互联网门户网站等相关服务器的对外开放服务。

- 对于特殊的应用，允许互联网移动办公公务员通过安全认证网关访问位于 DMZ 的业务应用。
- 禁止互联网用户访问内部网络应用系统。
- 关闭网络病毒相关端口，无特殊需要，禁止开放。
- 应对进出网络的数据流进行监控、分析和审计。
- 应阻止来自互联网的各种攻击。

3）核心网络与部门、分支结构网络的边界

核心网络与部门、分支机构网络的边界安全措施设计应符合以下要求：

- 中小型网络，不需要在该边界添加任何隔离设备。
- 大型网络，可根据需要，添加逻辑隔离设备（如防火墙或启用了过滤规则的路由器）。
- 应对进出核心局域网的数据流进行监控。
- 关闭网络病毒相关端口，无特殊需要，禁止开放。
- 允许核心网络访问部门或分支网络系统。
- 禁止核心网络的普通终端用户直接访问基础数据库服务子区域。
- 允许部门和分支网络用户在受控的前提下，访问核心网络中的服务器资源。

4）核心网络与异地容灾中心的边界

核心网络与异地容灾中心的边界安全措施设计应符合以下要求：

- 如采用数据级容灾，则不需要进行逻辑隔离，但是必须保护线路的物理安全。
- 如采用应用级容灾，则可以添加逻辑隔离设备，只允许开放远程数据存储和备份所需的相关服务。

3．路由交换设备安全配置

路由交换设备的安全配置应符合以下要求：

- 每台设备上要求安装经认可的操作系统，并及时修补漏洞。
- 路由器设置加长口令，网络管理人员调离或退出本岗位时口令应立即更换。
- 路由器密码不得以明文形式出现在纸制材料上，密码应隐式记录，记录材料应存放于保险柜中。
- 限制逻辑访问，合理处置访问控制列表，限制远程终端会话。
- 监控配置更改，改动路由器配置时，进行监控。
- 定期备份配置和日志。
- 明确责任，维护人员对更改路由器配置的时间、操作方式、原因和权限需要明确，在进行任何更改之前，制定详细的逆序操作规程。

4．防火墙安全配置

在不同的安全域之间或安全域内部不同安全级别的子区域之间可根据需要部署防火墙，防火墙的安全配置与路由交换设备基本相同，但是需要添加一项内容——防火墙

产品应有国家相关安全部门的证书。

5. 网闸安全配置

网络中如存在安全级别较高的区域，则可以通过网闸设备实施隔离；同时，网闸隔离尤其适用于工作性质较为特殊的单位，其内部网络中含有一定的敏感信息，可以通过网闸在受控的情况下与外部网进行连接。

网闸的安全配置要求同防火墙。

6. 入侵检测安全配置

入侵检测应符合以下要求：

- 中大型网络平台应部署基于网络的入侵检测系统（NIDS）。
- 网络入侵检测系统应对核心局域网、DMZ 区域进行检测。
- 如需要对大型网络的部门、分支机构网络进行入侵检测，应采用分布式方式部署入侵检测系统。
- 入侵检测产品应有国家相关安全部门的证书。
- 监控配置更改，改动入侵检测系统配置时，进行监控。
- 定期备份配置和日志。
- 入侵检测系统设置加长口令。
- 如采用分布式部署方式，各级入侵检测系统宜采用分级管理方式进行管理。

7. 抗 DDoS 攻击安全配置

抗 DDoS 攻击应符合以下要求：

- 网络平台应针对其对外提供服务的区域，例如 DMZ 区域部署抗 DDoS 设备。
- 抗 DDoS 攻击一般不部署于核心网络，而是部署于网络边界。
- 对于大型网络，可以采用独立的抗 DDoS 攻击设备，中小型网络可以采用带有抗 DDoS 攻击模块的防火墙或路由器产品。

8. 虚拟专用网（VPN）功能要求

无论是企业网络内多个局域网的 VPN 互连，还是提供外部网络用户访问内部网络的 VPN 网关，其技术要求都必须包括以下内容：

- 应提供灵活的 VPN 网络组建方式，支持 IPSec VPN 和 SSL VPN，保证系统的兼容性。
- 支持多种认证方式：支持用户名+口令、证书、USB+证书+口令三因素等认证方式。
- 支持隧道传输保障技术，可以穿越网络和防火墙。
- 支持网络层以上的 BPS 和 C/S 应用。
- 必须能够为用户分配专用网络上的地址并确保地址的安全性。
- 对通过互联网络传递的数据必须经过加密，确保网络其他未授权的用户无法读取该信息。

- 应能提供审计功能。

9．流量管理部署与功能要求

在带宽资源较为紧张的网络线路上，应可调节网上各应用类型的数据流量，调整和限定带宽，保证重要应用系统的网络带宽。通常情况下，流量管理设备部署于内部网络与互联网或者外部网络的出口处。流量管理应符合以下要求：

- 提供基于 IP 的总流量的控制。
- 提供多时段的网络流量统计分析。
- 提供网络实时负载分析。
- 提供关键业务流的实时流量监控。
- 提供应用流量带宽分配与控制。
- 提供用户分组管理，实现基于 IP 和基于用户的管理。

10．网络监控与审计部署与功能要求

网络监控与审计应符合以下要求：

- 应在核心网络中部署网络监控系统，采集和监控网络中的流量和事件、设备运行状况等信息，通过对这些信息的分析发现异常事件。
- 应实现对监控事件的实时性响应和多种方式的报警功能。
- 应实现对相关事件的关联处理、分析能力，实现对不良事件的应急处理能力。
- 应对异常事件及其处理进行审计。
- 提供对于审计中的异常信息建立相关的处理流程。

11．访问控制网络监控与审计部署与功能要求

访问控制应符合以下要求：

- 应在网络边界部署访问控制设备，启用访问控制功能。
- 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。
- 应对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制。
- 应在会话处于非活跃一定时间或会话结束后终止网络连接。
- 应限制网络最大流量数及网络连接数。
- 重要网段应采取技术手段防止地址欺骗。
- 应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。
- 严格限制拨号用户对网络不同区域的访问。

2.5.9.3 系统安全

1．身份认证

身份认证应符合以下要求：

- 登录系统时应当进行身份认证，并对此过程进行记录。
- 应定义认证尝试允许次数，并通过延长认证失败超出允许次数后再次允许认证的时间间隔来限制重复尝试，并对此过程进行记录。
- 用于身份认证的用户名和口令应在信道中加密传输。
- 应当对登录用户的来源进行控制和监控。
- 定期审计身份认证日志，对发现的异常行为进行及时处理，对累积性事件进行必要的趋势分析。

2．账户管理

账户管理应符合以下要求：

- 建立账户管理制度，负责系统账户的登记造册、用户名分配、初始口令分配、用户权限分配、系统资源分配、账户注销等，并定期检查系统中的账户分配情况，以及账户权限设置的正确性。
- 为不同用户分配不同的用户名或用户标识符，确保用户名或用户标识符具有唯一性。
- 用户名或用户标识符在系统内部全局唯一，在用户名或用户标识符被删除后，同名用户名或用户标识符不可再被创建。
- 记录用户的系统登录活动，定期审计和分析用户账户的使用情况，对发现的问题和异常情况进行相应处理。

3．主机系统配置管理

主机系统配置应符合以下要求：

- 应使用正版的操作系统软件。
- 不同的用户配备有不同的使用权限。
- 系统的目录与文件不能被远程用户“写/执行”共享。
- 限制服务器对外提供的服务资源，服务器不要求使用的远程端口应屏蔽/禁用。
- 运行时必须开启系统日志与审计功能。
- 不同用户的使用空间专用，且有磁盘空间限制。

4．漏洞与补丁发现系统

网络平台中应部署漏洞与补丁发现系统，或指定漏洞发现与补丁管理机制。漏洞发现与补丁管理应符合以下要求：

- 应定期采用专业化的工具进行系统漏洞扫描，及时发现漏洞，及时了解现有安全控制措施是否完备。
- 部署补丁管理软件对系统漏洞进行集中管理和控制，自动发现并下载最新的补丁

程序。

- 在有漏洞的主机上安装最新补丁程序，对可能危害计算机的漏洞进行及时修补。

5．内核加固

内核加固技术可抵御穿透防火墙和入侵检测系统的黑客攻击，补充防火墙等网络安全设备的不足。内核加固机制要求实现以下目标：

- 用户身份认证，实现系统管理员、安全管理员与审计管理员的三权分立。
- 区分用户的文件强制访问权限控制。
- 区分进程的文件强制访问权限控制。
- 文件强制访问权限控制。
- 区分进程的进程强制访问权限控制。
- 文件完整性保护。
- 服务完整性保护。
- 服务强制访问控制。
- 系统日志的安全保护。

6．病毒防护

病毒防护应符合以下要求：

- 防病毒软件的部署应该由点及面，全方位进行部署，彻底截断病毒入侵的途径。
- 在中小型网络平台中，可以采用扁平化方式部署病毒防护系统。
- 大型网络平台在病毒防护结构上应部署两级防病毒管理中心，采用三层体系架构方式。
- 两级病毒管理中心指在企业本部网络中建立一级系统中心，在分支机构网络中建立二级系统中心。
- 三层体系架构指防病毒系统整体架构应具有管理控制中心、管理控制台、杀病毒客户端的三层结构，以便有效地对防病毒系统进行管理控制和策略分发，其结构示意如图2-73所示。

7．桌面安全管理

桌面安全管理应强化对计算机终端状态、行为以及事件的管理，对网络上的每台计算机设备实施有效的接入管理、资产管理和安全管理。对于安全性要求较高的网络，桌面安全管理机制应符合以下要求：

- 桌面系统资源管理。
- 终端拓扑管理。
- 终端设备安全策略与接入管理。
- 设备行为与策略监控。
- 非法外联监控。

8．系统备份与恢复

系统备份与恢复应符合以下要求：

- 重要的系统必须实现确定的恢复功能，能够在出现故障时恢复到故障发生前的系统状态。

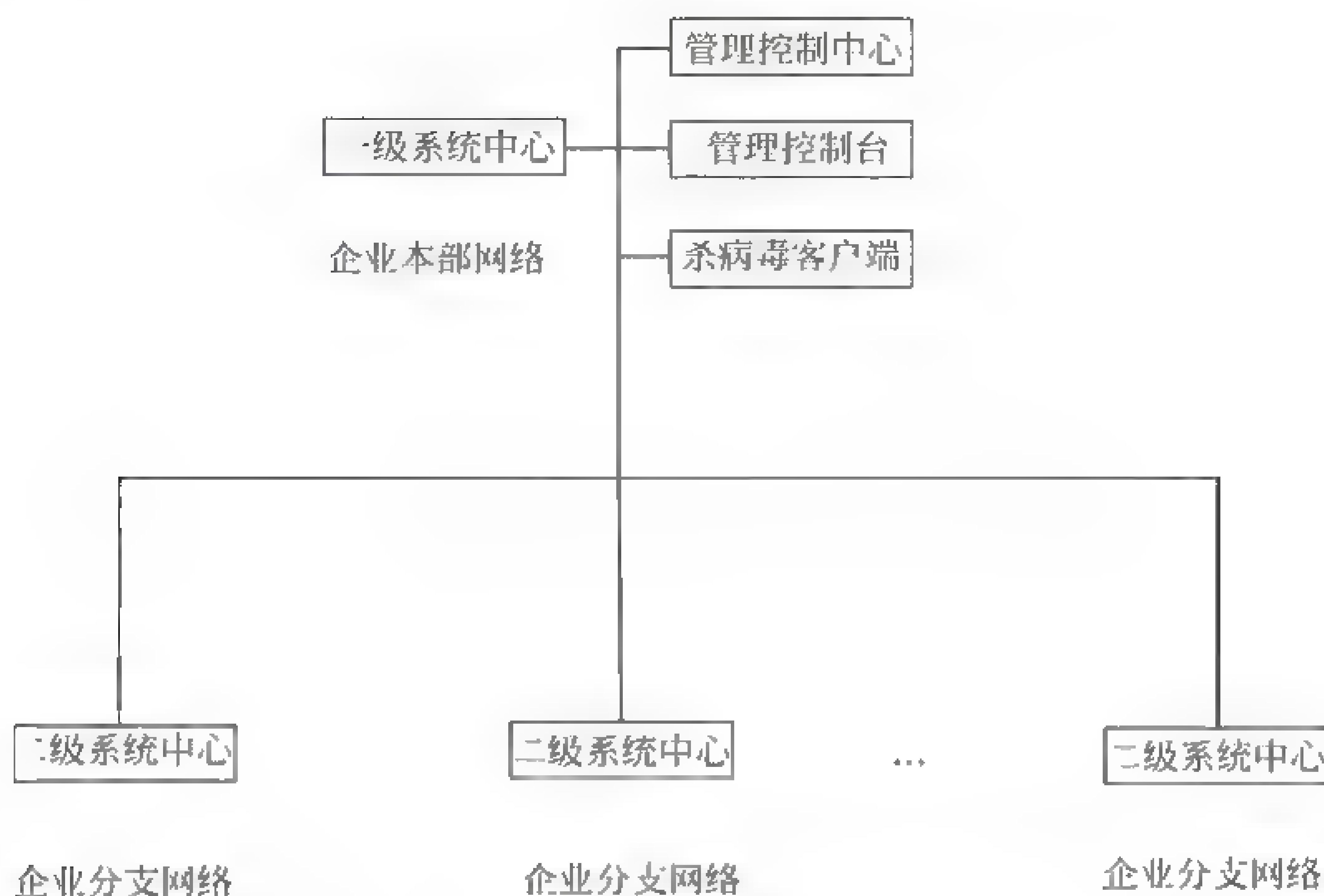


图 2-73　两级中心三层体系示意图

- 定期对全系统的完整运行现场进行备份。
- 对部分类型的服务中断，在无人工干预的情况下能使计算机网络系统恢复到安全状态，对其他的服务中断可由手动恢复实现。

9．系统监控与审计

对安全性要求较高的网络应制定系统监控与审计方案及相应的监控系统，系统监控与审计应符合以下要求：

- 对审计数据进行分析，包括分类、排序和趋势分析等。
- 对特定异常事件进行审计分析，提高实时报警功能。
- 支持集中审计和事件关联分析。
- 提供自动响应机制，如进行实时报警，终止违例进程，取消异常服务等。

10．访问控制

访问控制应符合以下要求：

- 应启用访问控制功能，依据安全策略控制用户对资源的访问。
- 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。
- 应实现操作系统和数据库系统特权用户的权限分离。
- 应严格限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认

口令。

- 应及时删除多余的、过期的账户，避免共享账户的存在。
- 应对重要信息资源设置敏感标记。
- 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

2.5.9.4 应用安全

1. 数据库安全

1）数据库访问控制

数据库访问控制应满足以下要求：

- 用数据库目录表、存取控制表、能力表等确定主体对客体的访问权限。
- 应允许命名用户以用户和/或用户组的身份规定并控制对客体的共享，并阻止非授权用户读取信息。
- 访问控制应与身份认证和审计相结合，通过确认用户身份的真实性和记录用户的各种成功的或不成功的访问，使用户对自己的行为承担明确的责任。
- 应限制授权传播，要求对不可传播的授权进行明确定义提供支持，由系统自动检查并限制这些授权的传播。
- 数据库用户的安全属性应在用户建立注册账号后由系统安全员进行标记，而客体的安全属性则以默认方式生成或由安全员通过操作界面进行标记。
- 将系统的常规管理、与安全有关的管理以及审计管理，分别由系统管理员、系统安全员和系统审计员来承担，按最小授权原则分别授予他们各自为完成自己所承担任务所需的最小权限，并在三者之间形成相互制约的关系。
- 数据库安全级别必须高于C2安全级别。
- 必须对数据库进行备份。

2）数据库中的身份认证

数据库中的身份认证访问控制应满足以下要求：

- 进入数据库系统的用户，首先应由支持数据库系统运行的操作系统进行身份认证。
- 当用户远程直接登录到数据库管理系统或与数据库服务器进行访问连接时，应进行用户认证。
- 本地登录用户，可以选择采用该用户在操作系统中的标识信息，也可以重新进行用户标识。重新进行用户标识应在用户注册（建立账号）时进行。
- 数据库管理系统用户标识一般使用用户名和用户标识（UID）。为在整个数据库系统范围实现用户的唯一性，应确保数据库管理系统建立的用户在系统中的标识（SID）与在各数据库系统中的标识（用户名或别名，UID 等）之间的一致性。
- 分布式数据库系统中，全局应用的用户标识信息和认证信息应存放在全局数据字

典中，由全局数据库管理安全机制完成全局用户的身份认证。局部应用的用户标识信息和认证信息应存放于局部数据字典中，由局部数据库安全机制完成局部用户的身份认证。

- 数据库用户的标识和认证信息应受到操作系统和数据库系统的双重保护。操作系统应确保任何用户不能通过数据库以外的使用方式获取和破坏数据库用户的标识和认证信息。
- 数据库系统应保证用户以安全的方式和途径使用数据库系统的标识和认证信息。
- 数据库用户标识信息应在数据库系统的整个生命期有效，被撤销的用户账号的 UID 不得再次使用。

3）数据库的安全审计

数据库的安全审计应满足以下要求：

- 应设计数据库审计功能，并应与用户标识与认证、自主访问控制、标记与强制访问控制等安全功能的设计紧密结合。
- 对与标识及强制访问控制等安全机制有关的内容，如安全属性的操作等进行审计。
- 对网络环境下运行的数据库管理系统，应建立分布式的审计系统，并由审计中心进行管理和控制。

4）数据库的容灾

数据库应考虑采用定期定时备份的方式进行容灾防护，备份的方式可以采用如下原则：

- 小型数据库可以采用基于磁带、磁盘文件的数据库备份方式。
- 中型数据库可以采用基于 SAN、NAS 技术的在线数据库备份方式。
- 大型数据库可以在基于 SAN、NAS 技术的在线数据备份方式之外，采用数据库应用级备份。

2．邮件服务安全

邮件安全系统防止邮件病毒、邮件炸弹和垃圾邮件进入网络内部，邮件服务的安全应达到如下技术要求：

- 能有效阻止恶意程序和病毒通过邮件进入网络。
- 能有效探测和记录各种垃圾邮件并过滤掉垃圾邮件。
- 能有效阻止恶意程序通过邮件进入网络。
- 邮件安全系统应具有国家相关安全部门的证书，否则不得投入使用。

3．Web 服务安全

1）网页防篡改

网页防篡改机制防止非授权人员随意篡改 Web 页面，对网页进行实时监控、保护。网页防篡改机制应满足以下要求：

- 一旦发生非法网页修改，系统应立即报警并进行恢复。
- 能够以多种形式（如电话、短信、邮件、铃声等）进行报警。
- 提供加密功能，杜绝传输过程中的信息篡改。

2）Web 日志审计

Web 日志审计是指记录和收集用户登录、浏览页面及其他相关操作的过程，它可以对破坏性行为提供有力证据。Web 日志审计应满足以下要求：

- 应定期进行日志审计并由专人负责。
- 确保审计数据的完整性和可读性。
- 保存对 Web 服务器的审计数据和分析结果，确保审计数据的可用性。
- 明确审计事件的处理流程。

3）Web 业务隔离

Web 业务隔离提供面向外部和面向内部的服务业务的独立性，防止出现问题时造成整体服务中断。技术要求应达到在面向外部用户的服务和面向内部用户的服务需求不同时，部署不同的服务器并进行逻辑隔离，分别对外部和内部提供服务。

4．应用系统的安全要求

1）对应用软件的基本要求

- 应用软件必须是正版软件。
- 未经认证的环境、工具，必须提交源设计代码，经相关专家组评价审定后，经现场编译后，方可使用。专家组成员必须是中国内地在政府机构、研究机构、企事业单位、大学等工作的信息安全方面的专家学者。
- 新开发应用软件运行时，必须保留人工工作方式至少半年，经认证无误后，方可停止人工工作；软件版本升级换代，必须对旧系统的数据进行必要的备份，并直接导入新系统，应该对新系统进行跟踪至少 3 个月。必要时，新软件正式运行前，应该经有关专家或者机构测试，确保正确无误。
- 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。
- 应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。
- 未经授权，不得用开发、管理工具直接远程连接到实际运行的网络设备、操作系统、数据库、中间件服务器等；授权连接操作结束后，必须尽快断开。

2）身份识别与认证

身份识别与认证应满足以下要求：

- 应用系统应采用基于数字证书的用户身份认证。
- 应用系统登录应该采用用户身份、口令验证，必要时应该加入验证码，防止恶意软件自动登录攻击。

- 应提供强制要求修改口令的功能。通过管理端的设置，可要求所有或部分用户必须定期或在符合特定条件的情况下修改口令。
- 应用系统应具有登录失败处理的功能，锁定登录失败次数超过一定数量的用户账号。
- 应用系统应具有超时处理的功能，当用户登录后在一段时间内无任何动作，应用系统应锁定界面并清除用户状态，用户必须再次进行身份认证才可恢复。
- 重要的应用系统，应该采用一次性口令密码。
- 不允许以超级用户的方式连接数据库系统、中间件服务器等，不允许使用超级用户访问操作系统、网络设备等。

3）数据的机密性和完整性保护

数据的机密性和完整性保护应满足以下要求：

- 应用系统的数据传输应基于数字证书的安全认证平台，通过 PKI/CA，对证书（密钥）和信任关系进行管理。
- 在应用软件通信过程中，对于敏感信息例如账号、密码、证件号码等字段采用事先约定加密算法进行加密。
- 采用事先约定的非对称加密算法加密摘要，形成数字签名。
- 在应用系统通信时，对整个应用报文或会话过程采用事先约定加密算法进行加密。对称加密算法的密钥通过非对称加密后进行传输。
- 重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时应采取必要的恢复措施。
- 重要业务数据在存储过程中完整性受到破坏，并在检测到完整性错误时应采取必要的恢复措施。

4）应用安全审计

应用安全审计应满足以下要求：

- 身份认证审核。
- 数据、文件的删除和修改等行为监控。
- 系统管理员、系统安全员、审计员和一般用户所实施的操作监控。
- 其他与系统安全有关的事件或专门定义的可审计事件。
- 对于每一个事件，其审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功，及其他与审计相关的信息。
- 日志信息应定期转存或备份到存储设备。
- 可对审计数据进行报表分析功能，包括分类排序、筛选、趋势分析。
- 应用系统可基于特定异常事件进行审计分析。
- 应用软件应支持将日志事件以某种通用格式输出，作为集中审计的输入。

5）访问控制

访问控制应满足以下要求：

- 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问。
- 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作。
- 应由授权主体配置访问控制策略，并严格限制默认账户的访问权限。
- 应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。
- 应具有对重要信息资源设置敏感标记的功能。
- 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

2.5.9.5 数据容灾与恢复

1. 总体要求

数据容灾机制保证企业网络核心业务数据在灾难发生后的及时恢复，数据容灾机制应符合以下总体要求：

- 有运行维护人员执行定期的数据备份任务。
- 有专门的运维人员定期检查数据备份情况。
- 应制定数据恢复预案，并由相关部门备案。
- 备份的数据必须有效且能进行恢复。

1）中小型网络数据容灾要求

中小型网络数据容灾在满足总体要求的基础上应做到：

- 拥有备用基础设施，备用基础设施可与省电子政务网共享。
- 拥有本地数据备份系统。

2）大型网络数据容灾要求

大型网络数据容灾在满足总体要求的基础上应做到：

- 应建立独立的备用基础设施。
- 应建立独立的数据备份系统。
- 应建立独立的备用数据处理系统。
- 应建立独立的备用网络系统。

2. 容灾系统建设

1）建设地址的选择

灾难恢复与灾难备份中心的建设地点应满足以下要求:

- 应与核心网络中心距离大于 10km。
- 网络基础设施较完善，能提供足够带宽的广域网络线路。
- 应能够提供充足的双回路电力保障。

- 不能在地震、洪涝、台风、雷击等地质灾害和天气灾害的多发地区。
- 不能在重要设施密集地区。
- 不能在交通要道附近。
- 不能与重要建筑和标志性建设相临。

2）基础建设的要求

备用基础设施包括支持灾难备份系统运行的机房、数据备份中心的存储基础设施和备份运行系统的服务器等。建设要求如下：

- 机房的建设应符合国标。
- 存储基础设施应建立有效的存储系统，以保证数据的安全性、备份的简单性和易管理性。
- 服务器应根据需要，针对核心网络中的主要服务，设立备份服务器。

3）网络线路的备份

备用网络系统包含备用网络通信设备和备用数据通信线路。应满足以下要求：

- 配备与核心网络相同等级的通信线路和网络设备，包括通信线路、路由器、交换机和防火墙等，使最终用户可通过网络同时接入主、备中心。
- 应部署一定的安全系统以保证容灾系统的安全，包括入侵检测等。

4）建设方式

数据备份系统设施的建设方式可采用单位自行建设、运行；多方共建或通过互惠协议获取；租用其他机构的系统，如商业化灾难备份中心的基础设施；事先与厂商签订紧急供货协议。

3. 数据备份与恢复

数据备份与恢复应满足以下要求：

- 应提供本地数据备份与恢复功能，完全数据备份应每天一次。
- 重要数据应定期从运行的系统中备份到本地的光盘、海量磁盘、磁带或磁带库等介质中。
- 应制定合理的备份策略。包括介质的分类、标记、查找方法；介质的使用、维护、保养、销毁；数据备份频率、保存时间等。
- 对数据备份策略的实施情况定期进行检查。
- 采用异地备份方式，数据可通过网络系统定时自动地备份到异地的磁盘阵列。
- 当某些因素引起数据不完整、不连续、不可靠、丧失业务的连续性或者数据库需要重建就应该进行业务数据的恢复。
- 数据恢复时，数据库管理员应填写数据恢复申请表，制订数据恢复计划报请主管批准。而后按恢复计划执行恢复操作。
- 业务数据恢复前的检查，即严格审查数据是否已经丧失连续生产的可能；严格审

查数据库是否需要重建；严格检查备份介质、备份数据是否有效。

- 对数据恢复工具进行严格控制，尽可能地防止误操作。并且数据的恢复工具应有详细的操作说明、操作步骤以及注意事项说明。

2.5.9.6 安全运维服务体系

1. 信息安全风险评估工作

1）风险评估的对象

安全风险评估的对象包括以下内容：

- 网络结构。
- 网络系统及设备。
- 应用系统。
- 管理制度。
- 人员意识与技能。
- 安全产品和技术应用状况。
- 安全事件处理能力。

2）评估方法

评估方法包括以下内容：

- 安全管理审计。
- 工具扫描。
- 网络架构评估。
- 应用系统评估。
- 主机设备和平台安全配置检查。
- 渗透测试和分析。

3）评估要求

安全风险评估服务是网络安全服务的一个重要环节，每年应进行一次信息安全风险评估。为避免出现重大的安全漏洞和隐患，可以在自行评估的基础上，定期或不定期地委托具备资格的信息安全风险评测机构进行评估。

2. 应急服务

1）应急响应

应急响应应达到以下要求：

- 设立应急响应中心，合理安排应急响应人员。
- 应针对各种可能情况制定合理的应急响应预案。
- 应制订详细合理的应急响应计划。

应急预案的执行单位可由网络管理中心相关部门执行，也可委托公司、大学或研究机构完成。受委托单位应是具有相关安全资质的中资机构。

2）应急预案的制定

为保证在发生各种信息安全事件情况下，能够从容处理并解决安全事件，要求制定应急预案。制定应急响应预案首先应建立应急处理工作小组，负责预案的落实，并且保证预案的传达与实施，应急预案要在相关部门或上级部门进行备案。预案的制定应符合以下要求：

- 应急预案应根据电子政务网实际情况制定，必须切实有效，可操作性强。
- 应急预案的制定和实施中明确各个部门的职责，责任落实到岗、到人。
- 确定应急事件的风险优先次序。对于高风险的应急事件，优先制定应急预案。
- 全面分析系统运行、信息内容和网络的管理与控制等方面的安全威胁。
- 完善应急预案所需的备用资源，包括备用的软件、设备以及人员。
- 每种应急事件建立应急响应流程。
- 当不能判断事件发生原因时，一定要保留现场，保留痕迹，追查原因。
- 重大事件要上报有关部门，直至追究行政或刑事责任。
- 对预想到的事件要事先积极采取管理和技术措施，尽早解决。
- 应急预案应经常进行培训和演练。

3）应急预案的内容

应急预案的内容应包括以下内容。

- 标题：包括应急事件的名称、事件编号以及事件处理的优先等级。
- 事件描述：包括应急事件发生的背景、现象、可能的影响以及影响范围。
- 涉及范围：包括应急处理工作组人员与部门职责。
- 处理概述：包括描述事件处理主要环节和要点。
- 处理流程：包括用流程图简述处理过程。
- 流程说明：包括针对流程图每个步骤，详细描述涉及的具体人员、操作对象（如设备端口号、IP 地址、主机名、文件名、备份介质编号与存放地点等）、操作命令、使用的工具等。
- 演练计划：包括预演环境的建立、参与人员、时间与地点，对上述处理流程进行实际操作、验证预案的合理性，增强事件处理的熟练程度与可靠性。
- 参与人员：包括编制人、预案人与审批人，以及需要抄送的部门。

4）应急预案的流程

安全事件应急处理的标准流程如图 2-74 所示。

5）应急响应步骤

应急响应步骤是安全事件或事故发生后应急中心根据应急预案进行更具体的应急响应步骤。当入侵或破坏发生时，对应的处理步骤如下。

（1）保护或恢复计算机、网络服务的正常工作，进行应急准备。

① 为一个突发事件的处理取得管理方面的支持。

② 组建事件处理队伍（1～10人）。

③ 提供易实现的初步报告。

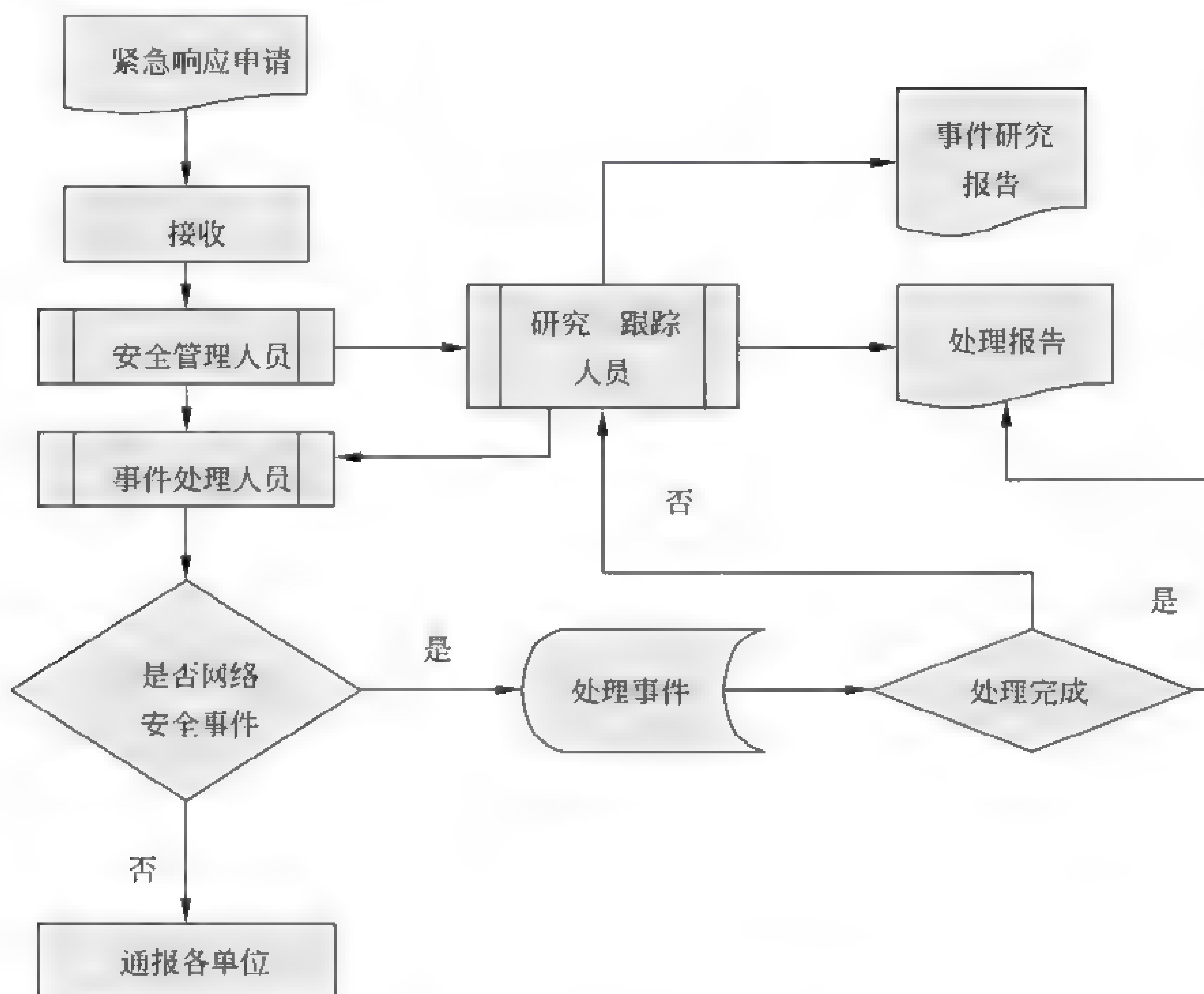


图 2-74 应急预案的标准流程

（2）追查入侵者，识别事件（判定安全事件类型）。

① 初步评估，确定事件来源。

② 保护可追查的线索，立即在磁带上或其他不联机存储设备上备份日志数据。

（3）抑制缩小事件的影响范围。

① 确定系统继续运行的风险如何，决定是否关闭系统及其他措施。

② 根据需求制定相应的应急措施。

（4）解决、恢复以及跟踪问题。

① 事件的起因分析、取证追查。

② 漏洞分析、后门检查。

③ 提供解决方案、结果提交专家小组或上级领导审核。

（5）后续工作。

① 检查是不是所有的服务都已经恢复。

② 攻击者所利用的漏洞是否已经解决。

③ 其发生的原因是否已经处理。

④ 保险措施、法律声明等手续是否已经归档。

⑤ 应急响应步骤是否需要修改。

⑥ 生成紧急响应报告。

⑦ 拟定一份事件记录和跟踪报告。

⑧ 录入专家信息知识库。

3．安全监控与管理服务

1）部署要求

安全监控与管理是通过统一集中的安全管理机制来总体配置、调控整个网络多层面、分布式的安全系统，提高安全预警能力，加强安全应急事件的处理能力。应符合以下要求。

（1）以分布式的体系架构来实现监测和管理功能，在省电子政务网核心局域网以及市州政务网络中心分别部署两级监控管理中心。

（2）每一级设置独立的数据库，下级网管能够主动或被动地将部分或全部数据上传到上级系统。

（3）上级管理节点能对下级管理节点进行配置和监测数据同步，支持上级管理节点对下级管理节点的远程管理。

（4）管理功能集成于一个管理平台，统一于一个管理图形界面。

（5）可监测和管理网络、应用系统和运行环境，形成一套统一的网络与应用系统状态管理体系。

2）监控功能要求

监控功能应符合以下要求。

（1）应能够采集网络设备、安全设备、服务器和应用系统等的运行状态、性能、故障和事件信息。

（2）应能对安全事件进行过滤、关联分析和告警。

（3）应能对网络、主机、数据库、中间件、安全设备和应用系统等 IT 资产进行集中统一管理。

（4）安全事件处理和风险分析功能。

（5）可以统计分析所有事件、风险、通知、资产和其他资源，能够创建报表。

3）管理功能要求

管理功能应符合以下要求。

（1）运行值班管理。

（2）事件告警处理。

（3）运行维护管理。

（4）设备辅助信息管理。

（5）事件统计与运行考核管理。

（6）告警事件处理知识管理。

4）规模要求

大型网络需要部署安全监控与管理平台，中型网络的核心网络需要部署安全监控与管理平台。

4．其他安全服务

（1）定期安全巡检。大中型网络中应每月进行一次巡检，旨在发现系统运行过程中是否有新的风险出现，确定修补的方案，并对系统进行加固。

（2）安全加固服务。应当对网络平台中的重要应用服务器定期进行安全加固服务。加固之前需要进行安全评估，并针对安全评估后的结果修补系统的漏洞，加强系统的安全配置，进行全面系统的加固工作。大中型网络宜每季度进行一次，而小型网络每半年进行一次。

（3）安全信息通告服务。网络平台，尤其是大型网络平台，应进行定期的安全信息通告服务。安全信息中应包括最新的安全公告、病毒信息和漏洞信息等内容。安全通告服务以邮件、电话和走访等方式，将安全技术和安全信息及时传递给客户。

（4）安全培训。建立信息安全保障体系还要注重信息安全人才的教育与培养。信息安全的保障是靠人、技术和管理共同来实现的，人员的安全意识和安全技术水平将直接影响到整个信息安全系统的有效利用。

2.5.9.7 安全管理体系

1．安全管理体系框架

常见的安全管理体系框架如图 2-75 所示。

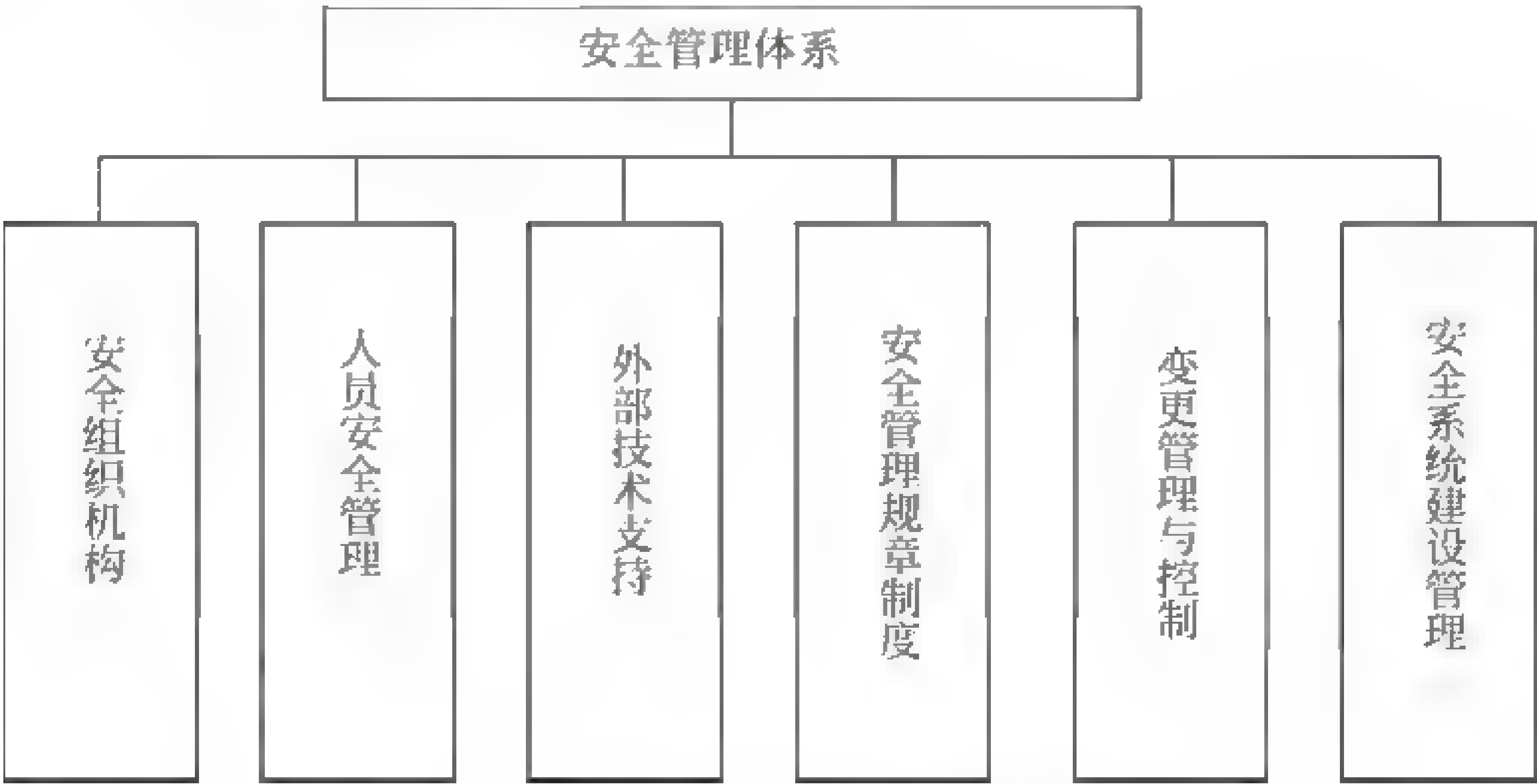


图 2-75 常见的安全管理体系框架

2．建立安全组织机构

网络平台应建立信息安全领导小组，该小组是信息安全的最高决策机构。信息安全

领导小组内应明确指定专人负责信息安全工作、应急处理工作和安全保卫工作。

信息安全管理机构是负责信息安全的职能部门。

3．人员安全管理

1）信息安全人员的基本要求

（1）信息安全管理人员（以下称信息安全人员）应当政治过硬、业务素质高、遵纪守法、恪尽职守。

（2）信息安全管理机构人员应具有相关专业技术背景、工作经历和一定的信息安全资质等。

（3）违反国家法律、法规和行业规章受到处罚的人员，不得从事信息安全管理工作。

2）信息安全人员的管理要求

（1）应配备适当数量的信息安全人员。

（2）应建立相关信息安全人员管理制度，并负责对信息安全人员的管理。

（3）信息安全人员应相对固定，以保持工作的延续性。

3）信息安全人员的职责范围

负责信息安全管理的日常工作。

（1）开展信息安全检查工作，对要害岗位人员安全工作进行指导。

（2）开展信息安全知识的培训和宣传工作。

（3）监控信息安全总体状况，提出安全分析报告。

（4）了解行业动态，为改进和完善信息安全管理工作，提供安全防范建议。

（5）及时向信息安全工作领导小组和有关部门、单位报告信息安全事件。

4）第三方人员管理

第三方人员包括软件开发商、硬件供应商、系统集成商、设备维护商、服务提供商和临时工。对第三方人员的访问应进行监控和审计，对第三方人员的权限应该严格控制和检查，对第三方人员的依赖程度应该能够控制并有补救措施。通常应做到如下几点。

（1）信息系统应对第三方人员的物理访问和逻辑访问实施访问控制，根据其在系统中完成工作的时间、性质、范围和内容等方面的需要给予最低授权。

（2）第三方人员的现场工作或远程维护工作内容应在合同中明确规定，如工作涉及敏感信息内容，应要求其签署保密协议。

（3）一般情况下，第三方人员的现场工作，如数据库、系统、因特网扫描；入侵检测；白客渗透以及其他软件的安装等不许接入自带的设备。

（4）第三方人员的现场工作应在有关人员的陪同和监督下完成。第三方人员自带设备与生产系统的接入应得到特别授权，其操作应受到审计。

（5）第三方人员工作结束后，应及时清除有关账户、过程记录等信息。

4．外部技术支持

外部技术支持包括聘请外部信息安全顾问，委托具备资质的单位负责安全管理等。

外部信息安全顾问的职责如下。

(1) 对信息安全管理小组在安全策略制定方面提供帮助。

(2) 帮助对安全系统项目建设、日常安全管理和控制、应用系统的安全管理和维护工作提供技术建议。

(3) 对安全事故的处理决策提供建议。

5. 安全管理规章制度

设计人员在针对网络制定规章制度时，可参照下述的几个方面，根据当地实际情况制定具体的安全管理规章制度。

1) 资产安全管理

(1) 应有“信息资产的分类和标识管理办法”，主要内容包括信息资产分类的定义，信息资产访问控制权限，信息资产的数据保护，信息资产的管理和使用等。还应说明信息所属信息资产分类，以及本系统信息资产的存放形式等。

(2) 应有“软硬件设备管理制度”，主要内容包括设备购置、设备管理、设备应用、设备维护和维修及设备报废等。

2) 运行维护管理

(1) 应有“机房安全管理制度”，主要内容应包括机房安全管理、机房卫生管理、机房设备管理和介质安全管理等。

(2) 应有“防病毒管理制度”，主要内容应包括病毒定义、组织领导和机构人员、防病毒管理员工作要求、防病毒管理员工作程序及一般用户的防病毒要求等。

(3) 应有“网络及系统运行安全管理制度”，主要内容应包括网管人员职责、网络运行管理和网络设备管理等。还应建立网络访问控制授权审批表、网络运行维护和应急处理记录等。

6. 变更管理和控制

变更管理和控制应符合以下要求。

(1) 目标是确保变更实施过程受到控制，对各项变化内容进行记录，保证变更对业务的影响最小。

(2) 变更内容审核和审批：对变更目的、内容、影响、时间和地点以及人员权限进行审核，以确保变更合理、科学地实施。按照机构建立的审批流程对变更方案进行审批。

(3) 建立变更过程日志：按照批准的变更方案实施变更，对变更过程各类系统状态、各种操作活动等建立操作记录或日志。

(4) 形成变更结果报告：收集变更过程的各类相关文档，整理、分析和总结各类数据，形成变更结果报告并归档保存。

7. 安全系统建设管理

1) 安全方案设计

安全方案设计应包括以下内容。

（1）应根据系统的安全保护等级选择基本安全措施，并依据风险分析的结果补充和调整安全措施。

（2）应指定和授权专门的部门对信息系统的安全建设进行总体规划，制订近期和远期的安全建设工作计划。

（3）应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件。

（4）应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后才能正式实施。

（5）应根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案等相关配套文件。

2）安全产品采购和使用

安全产品采购和使用应符合以下要求。

（1）应确保安全产品采购和使用符合国家的有关规定。

（2）应确保密码产品采购和使用符合国家密码主管部门的要求。

（3）每一个网络平台，其同一类别的安全产品原则上应采用同一品牌的产品。

3）安全服务商选择

安全服务商选择应符合以下要求。

（1）应确保安全服务商的选择符合国家的有关规定。

（2）安全服务商应具备国家相关部门颁发的安全服务资质证书。

（3）应与选定的安全服务商签订与安全相关的协议，明确约定相关责任。

（4）应与选定的安全服务商签订与安全相关的保密协议，明确保密义务。

2.5.10　编写逻辑设计文档

逻辑设计文档是所有网络设计文档中技术要求最详细的文档之一，该文档是需求、通信分析到实际的物理网络建设方案的一个过渡阶段文档，但也是指导实际网络建设的一个关键性文档。在该文档中，网络设计者针对通信规范说明书中所列出的设计目标，明确描述网络设计的特点，所制定的每项决策都必须有通信规范说明书、需求说明书、产品说明书以及其他事实作为凭证。

编写逻辑设计文档必须使用非技术性描述的语言，并与客户就业务需求详细讨论网络设计方案，从而设计出符合用户需要的网络方案。

在正式编写逻辑网络设计文档之前，需要进行数据准备。例如，需求说明书、通信规范说明书、设备说明书、设备手册、设备售价、网络标准以及其他设计者在选择网络技术时所用到的信息等，这些可能都是逻辑设计阶段需要的原始数据。虽然逻辑设计文档只包含其中的一小部分数据，但是与所有的原始数据一样，应当对这些数据进行有条

理的整理，以便以后查阅。

逻辑设计文档对网络设计的特点及配置情况进行了描述，它由下列主要元素组成。

（1）主管人员评价。

（2）逻辑网络设计讨论。

（3）新的逻辑设计图表。

（4）总成本估测。

（5）审批部分。

（6）修改逻辑网络设计方案。

2.5.10.1 主管人员评价

主管人员需要对项目进行概述，其内容如下。

（1）简短描述项目。

（2）列出项目设计过程各阶段的清单。

（3）项目各个阶段目前的状态，包括已完成的阶段和正在进行的阶段。

除了上述这些要点外，还应回顾一下双方已经达成共识的需求分析说明书和通信规范说明书。

2.5.10.2 逻辑网络设计讨论

当网络设计者讨论逻辑设计时，应当将重点放在要解决的问题上，而不是解决问题所用的工具上。因此，逻辑设计文档应着眼于通信规范中的设计目标，并给出每个目标实现的技术方案。

设计目标讨论的内容包括以下方面。

（1）具体设计目标。描述设计目标实现的关键数据。

（2）提出解决方案。为了排除故障或满足商业需求，详细阐述设计目标的实现方案。解决方案中要说明是否需要使用现有设备、购置新设备或者两者都需用。

（3）成本估测。虽然在物理设计尚未完成之前，不可能做出精确的成本估测，但是也要尽可能地对每种方法的技术成本做出估测，以确定设计方案是否超出了预算。

2.5.10.3 新的逻辑设计图表

正如用通信规范说明书了解当前网络状况一样，逻辑网络设计必须能清晰地表明新网络的特点及所需要的配置情况，包括新设备、链路或实施安全级别等，图表应当清晰表示出新网络和现有网络的区别。

2.5.10.4 总成本估测

要想得到新技术总的成本估价，可以将各个独立方案的成本组合在一起。注意，要

考虑一次性成本和需要重复支出的成本。此外，还要考虑包含新的培训成本、咨询服务费用以及雇用新员工等在内的成本。

如果提出的方案成本估算已经超出了预算，那么要把方案在商业上的优点列出来，然后提出一个满足预算的替代方案。

如果方案成本估算在预算的范围内，就不用缩减预算了，但要提醒管理者安装成本还是必须要考虑到最后的预算之中。

2.5.10.5　审批部分

在方案物理设计阶段开始前，逻辑设计方案必须经过高层人员审批。逻辑设计方案通过批准，管理层同意接受提出的功能性解决方案，同时获得相应的实现技术。

最后，为使文档生效，需要各个管理者在逻辑设计文档说明书上签名，网络设计组代表也要签名。

2.5.10.6　修改逻辑网络设计方案

对于每次的修改，需要保存好修改的备份、后继版本号，包括在文档开始前概述中的版本及修改的注释等信息。

2.6　物理网络设计

物理网络设计是网络设计过程中，紧随逻辑网络设计的一个重要设计部分，通过对逻辑网络设计的物理化，提供了网络实施所必需的信息。物理网络设计的输入是需求说明书、通信规范说明书和逻辑网络设计说明书。

物理网络设计的任务是为所设计的逻辑网络设计特定的物理环境平台，主要包括结构化布线系统设计、机房环境设计、设备选型和网络实施，这些内容要有相应的物理设计文档。由于逻辑网络设计是物理网络设计的基础，因此逻辑网络设计的商业目标、技术需求和网络通信特征等因素都会影响物理网络设计。

2.6.1　结构化布线设计

2.6.1.1　基本概念

结构化布线系统是一个能够支持任何用户选择的话音、数据、图形图像应用的电信布线系统。系统应能支持话音、图形、图像、数据多媒体、安全监控和传感等各种信息的传输，支持 UTP、光纤、STP 和同轴电缆等各种传输载体，支持多用户多类型产品的应用，支持高速网络的应用。

结构化布线系统具有以下特点。

（1）实用性。支持多种数据通信、多媒体技术及信息管理系统等，适应现代和未来技术的发展。

（2）灵活性。任意信息点能够连接不同类型的设备，如计算机、打印机、终端和服务器等。

（3）开放性。能够支持任何厂家的任意网络产品，支持任意网络结构，如总线型、星型和环型等。

（4）模块化。所有的接插件都是积木式的标准件，方便使用、管理和扩充。

（5）扩展性。实施后的结构化布线系统是可扩充的，以便将来有更大需求时，很容易将设备安装接入。

（6）经济性。一次性投资，长期受益，维护费用低，使整体投资达到最少。

2.6.1.2 系统构成

结构化布线系统分为 6 个子系统：工作区子系统、水平布线子系统、干线子系统、设备间子系统、管理子系统和建筑群子系统，如图 2-76 所示。

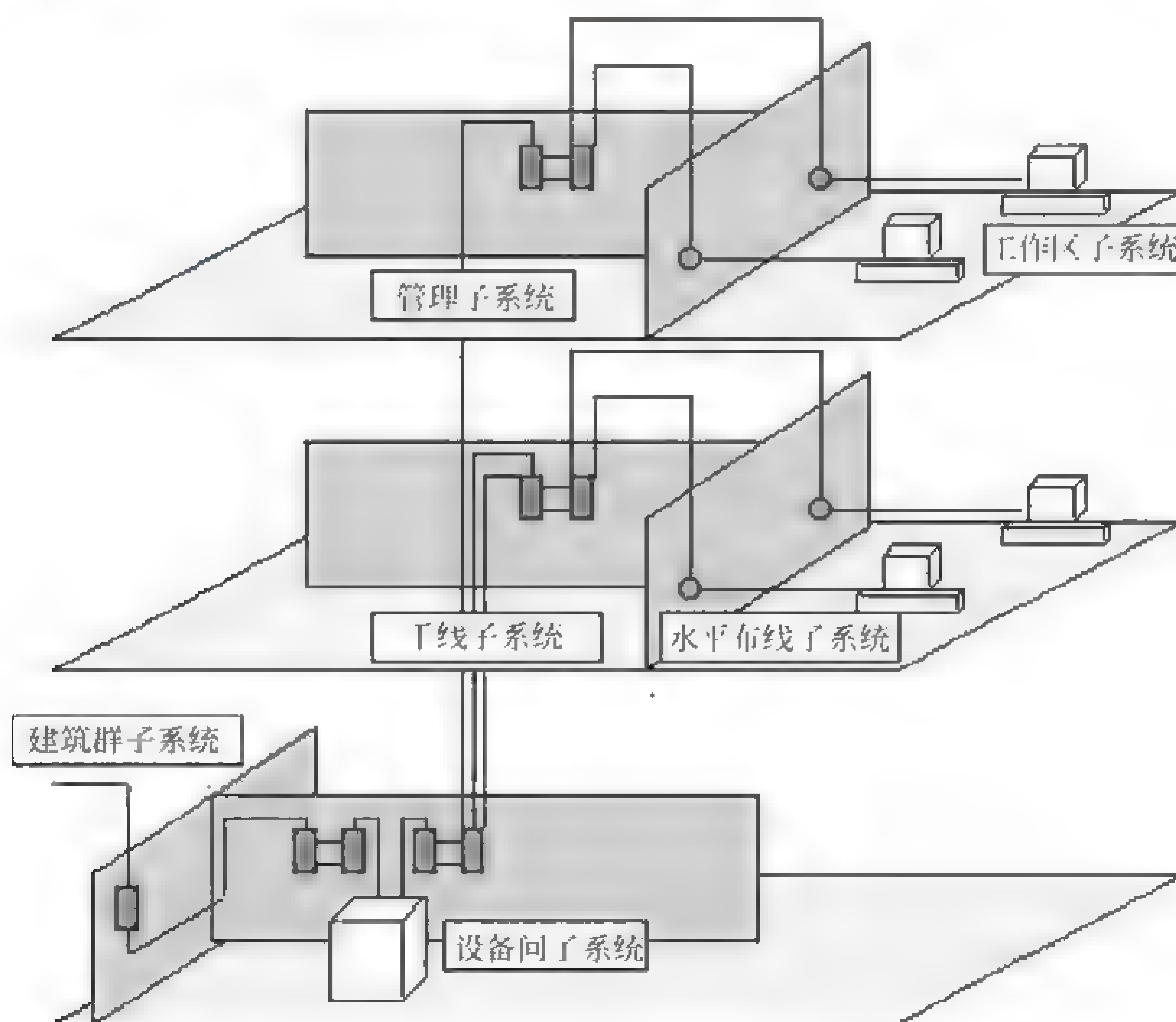


图 2-76 结构化布线系统示意图

1．工作区子系统

工作区子系统由终端设备连接到信息插座的连线（或软线）组成，包括装配软线、

适配器和连接所需的扩展软线，并在终端设备和 I/O 之间搭桥，如图 2-77 所示。

2．水平布线子系统

水平布线子系统的作用是将干线子系统线路延伸到用户工作区。水平布线子系统与干线子系统的区别是：水平布线子系统处于同一楼层，并端接在信息插座或区域布线的中转点上；水平布线子系统一端端接于信息插座上，另一端端接在干线接线间或设备机房的管理配线架上，如图 2-78 所示。

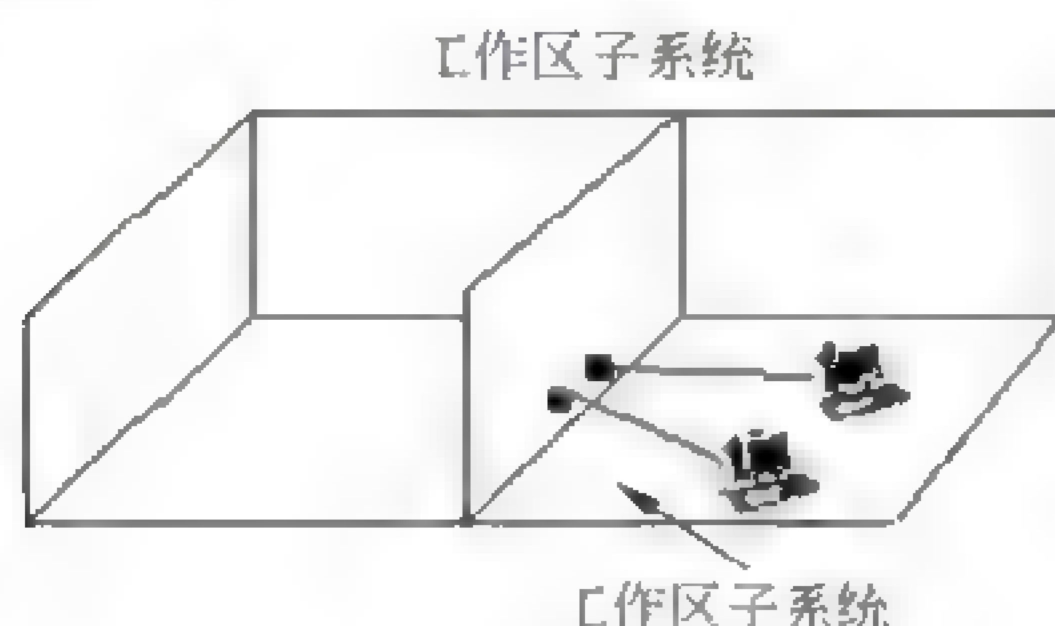


图 2-77　工作区子系统

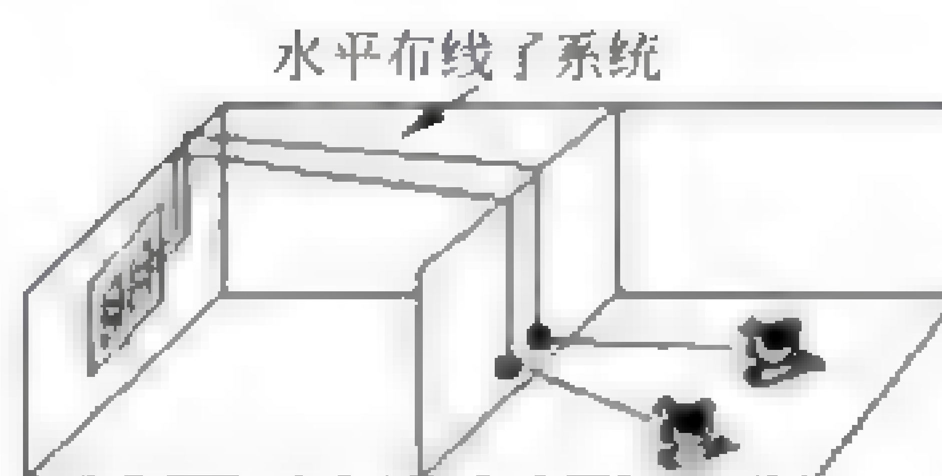


图 2-78　水平布线子系统

3．管理子系统

管理子系统由交连、互连配线架和信息插座式配线架以及相关跳线组成。管理点为连接其他子系统提供连接手段，交连和互连允许将通信线路定位或重新定位到建筑物的不同部分，以便能更容易地管理通信线路。

通过卡接或插接式跳线，交叉连接允许将端接在配线架一端的通信线路与端接于另一端配线架上的线路相连。插入线为重新安排线路提供一种简易的方法，而且不需要安装跨接线时使用的专用工具，如图 2-79 所示。

4．干线子系统

干线子系统是建筑物内网络系统的中枢，实现各楼层的水平子系统之间的互联。干线子系统提供建筑物的干线（馈电线）电缆的路由，通常由垂直大对数铜缆或光缆组成，一端端接于设备机房的主配线架上，另一端通常端接在楼层接线间的各个管理分配线架上，如图 2-80 所示。

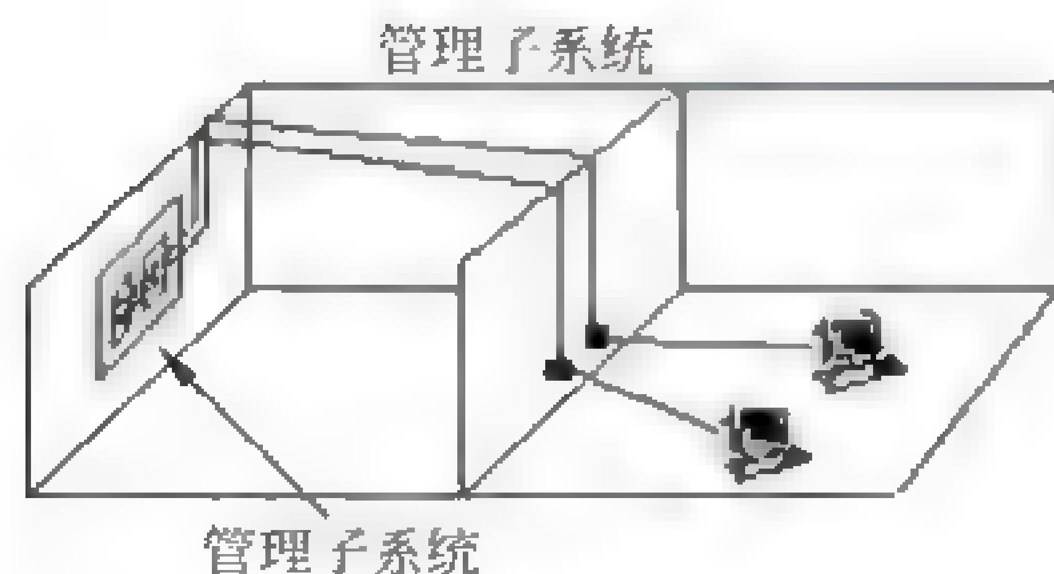


图 2-79　管理子系统

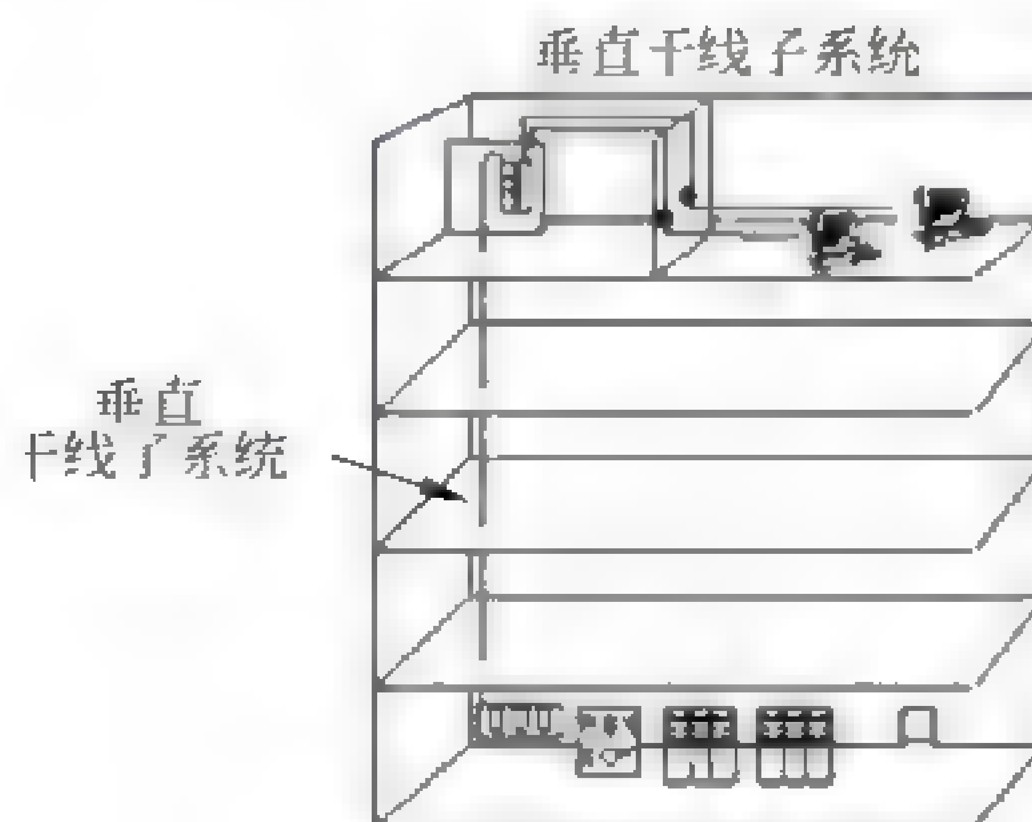


图 2-80　干线子系统

5. 设备间子系统

设备间子系统由设备中的跳线电缆、适配器组成，实现中央主配线架与各种不同设备的互连，如 PBX、网络设备和监控设备等与主配线架之间的连接。通常设备间子系统设计与网络具体应用有关，相对独立于通用的结构布线系统，如图 2-81 所示。

6. 建筑群子系统

建筑群子系统将一个建筑物中的电缆延伸到建筑群的另外一些建筑物中的通信设备和装置上。该子系统是整个布线系统中的一部分，并支持提供楼群之间通信设施所需的硬件，其中有导线电缆、光缆和防止电缆的浪涌电压进入建筑物的电气保护设备，如图 2-82 所示。

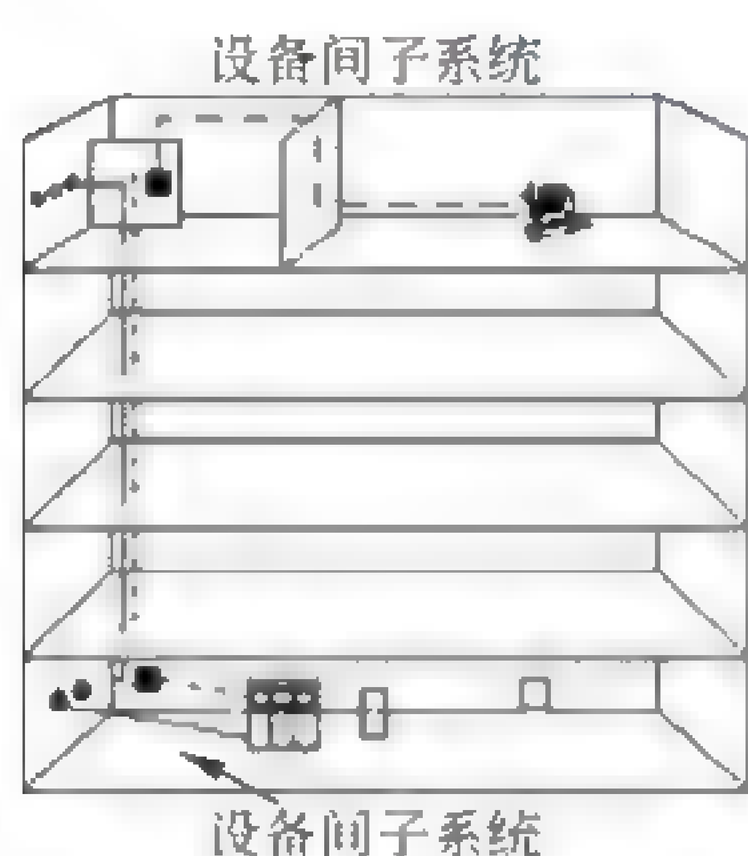


图 2-81 设备间子系统

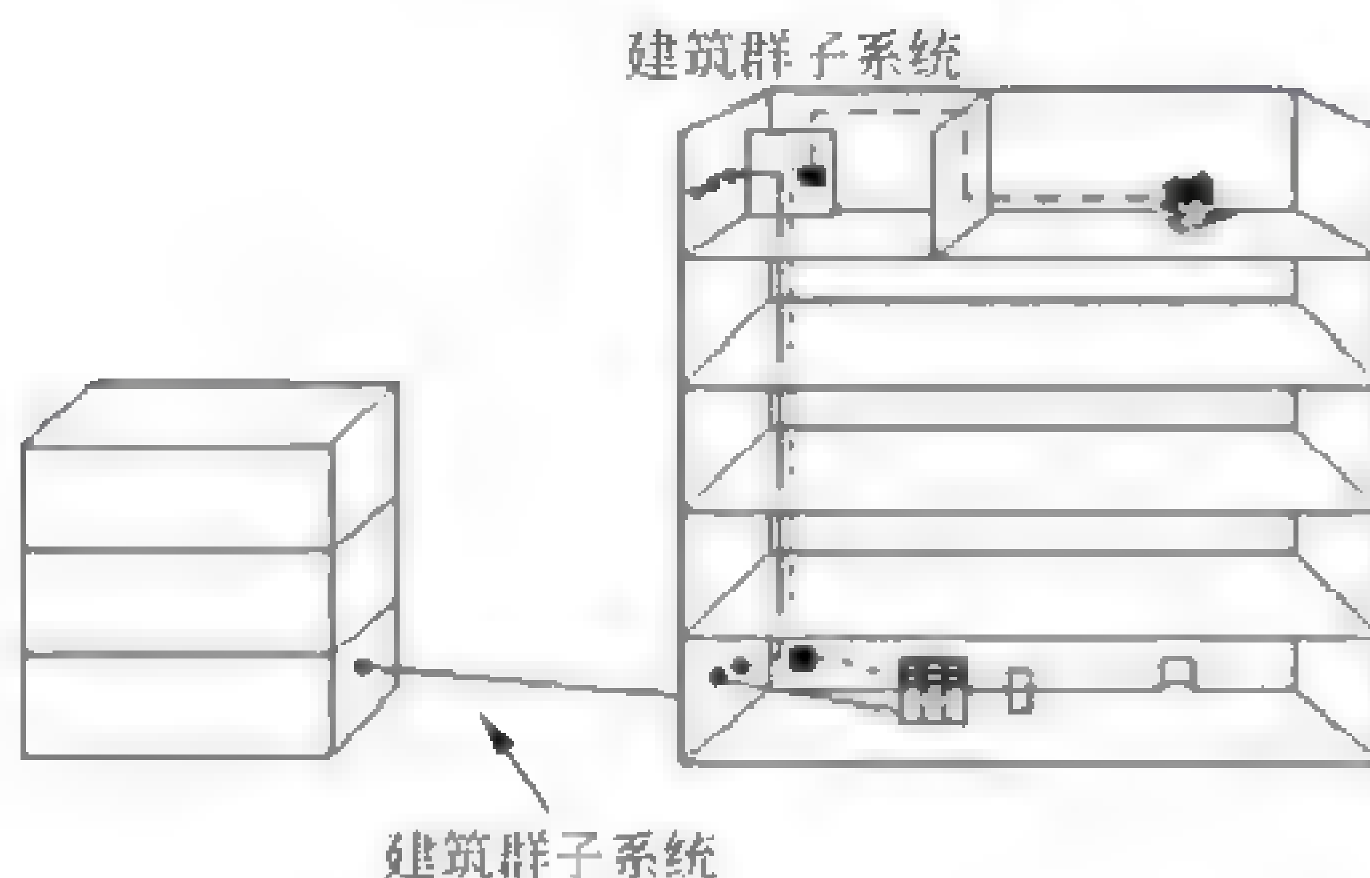


图 2-82 建筑群子系统

2.6.1.3 设计要点

1. 工作区子系统设计要点

工作区子系统的布线通常是非永久性的，但在设计阶段可根据用户的需要增加或改变，既便于连接也易于管理。工作区子系统中的信息插座类型选择应根据网络系统的规模和终端设备的种类、数量而定。

工作区子系统中的布线、信息插座通常安装在工作间四周的墙壁下方，也有的安装在用户的办公桌上，而无论安装在何处，应以方便、安全、不易损坏为目标。

工作区子系统的布线，实质上相当于通信线路的布线，终端包括计算机、电话机、传真机和有线电视机等设备，应使这些终端设备与信息插座（通信引出端）相连。

2. 水平布线设计要点

在进行水平布线时，传输媒体中间不宜有转折点，两端应直接从配线架连接到工作区插座。水平布线的布线通道有两种：一种是暗管预埋、墙面引线方式；另一种是地下管槽、地面引线方式。前者适用于多数建筑系统，一旦铺设完成，不易更改和维护；后者适合于少墙、多柱的环境，更改和维护方便。

3．管理子系统设计要点

对于楼层较少的楼栋来说，管理子系统可以不采用配线间的方式，而是采用悬挂式配线柜。

对于大多数楼栋来说，每一楼层至少有一个配线间，用于放置交换机、集线器和配线架等交叉连接设备。配线架等交叉设备通过水平布线子系统连接至各工作区的信息插座。集线器或交换机与交叉设备之间通过短线缆互连，这些短线被称为跳线。通过跳线的调整，可以方便地形成工作区的信息插座和交换机端口的连接切换。

同时，干线子系统将根据其分布式结构独立地连接到每一个配线间，大多数情况下，管理子系统的配线间至少拥有一条以上的主干线缆。

4．干线子系统设计要点

干线子系统在设计时，对于旧式建筑，主要采用楼层牵引管等方式铺设；对于新式建筑物，主要利用建筑物的线井进行铺设。

5．设备间子系统设计要点

设备间子系统是一幢建筑物中集中存放的各种设备，如主机、电话专用程控交换机、调制解调器的安放柜、网络服务器和局域网络集线器等。就结构化局域网而言，这种设备间应包括一个主要的交叉连接器。

在选择设备间位置时，既要考虑到连接方便的要求，也要兼顾对电磁干扰的要求。考虑到结构化布线的投资、施工安装与维护等，设备室通常选择在一幢建筑物的中部楼层。设备室的供电要求也格外严格，通常要配备不间断电源，还要有备份电源。

6．建筑群子系统设计要点

建筑群子系统主要由连接楼栋的线缆构成，在设计时，应尽量使用地下管道铺设方式，管道内铺设的铜缆或光缆应遵循电话管道和入孔的各项设计规定。此外，安装时至少应预留 1~2 个备用管孔，以供扩充之用。

建筑群子系统采用直埋沟内铺设时，如果在同一个沟内埋入了其他的图像、监控电缆，应设立明显的共用标志。

2.6.1.4 布线距离

在进行结构化布线系统设计时，需要注意到线缆长度对布线设计的影响。表 2-17 是 EIA/TIA-568 标准提出的常用的布线距离的最大值。

表 2-17 布线距离

子　系　统	光纤(m)	屏蔽双绞线(m)	非屏蔽双绞线(m)
建筑群（楼栋间）	2000	800	700
主干（设备间到配线间）	2000	800	700
配线间到墙上信息插座		90	90
信息插座到网卡		10	10

另外，由于高速以太网对双绞线的距离限制，大多数情况下，建筑群、干线子系统的双绞线等线缆主要用于电话、报警信号等。网络信号基本都不再使用双绞线，而是由光纤进行替代。

2.6.1.5 线缆铺设准则

铺设线缆的质量会影响到网络的工作性能，在铺设线缆时要注意以下方面。

（1）应充分考虑线缆的冗余，以备扩展需要，尤其是新建的楼栋。线缆的扩容铺设成本要远远大于初期铺设的冗余成本。

（2）铺设线缆时应遵循国家和政府在建筑方面的政策方针，在铺设之前，应该确认铺设计划是否符合结构化布线铺设的条文规定。

（3）应聘请经验丰富的布线铺设承包商来完成铺设工作。

（4）铺设之前应测试线缆设备以保证要铺设的线缆都满足需要的性能指标。

（5）对于线缆需要经过压力通风系统时，应该使用压力通风型线缆，该种线缆具有外层绝缘皮，在阻燃的同时不会产生毒烟。例如，在支撑天花板的上方，散热通气孔、通风道以及空调系统的环境下，就要求使用这种特殊质量的线缆。

（6）对所有不同类型的线缆进行整理，并制订出线缆、设备和连接器维护计划。

（7）一般情况下，不要剥掉线缆外面的塑料，不要将绞在一起的线缆末端分开，除非连接时必须要这样做；否则，可能会导致额外的串音。

（8）确保线缆质量，并选用正确等级的线缆来铺设。

（9）尽可能地让数据线垂直通过电力线。

（10）不要近距离（小于15～20cm）平行铺设铜质电线和电力线。应该让数据线与电力线保持几米远的距离。

（11）使用挂钩来固定天花板上的线缆。

（12）保证线缆末端尽可能短，以防噪声干扰。

（13）保证每个系统之间处于良好连接的状态，应有过压保险和照明保护，此外还要铺设不间断电源。

2.6.2 机房设计

机房的设计应参照 GB 50174—1993《电子计算机机房设计规范》，需要遵循的设计要求如下。

2.6.2.1 机房位置及设备布置

1．中心机房位置选择

（1）中心机房的物理位置在多层建筑或高层建筑物内宜设于第1～8层，更高层次不适合作为机房建设楼层。

（2）机房位置选择应符合以下要求。

① 水源充足、电力比较稳定可靠、交通通信方便、自然环境清洁。

② 远离产生粉尘、油烟、有害气体以及生产或储存具有腐蚀性、易燃、易爆物品的工厂、仓库、堆场等。

③ 远离强振源和强噪声源。

④ 避开强电磁场干扰。

（3）当无法避开强电磁场干扰或为保障计算机系统信息安全，可采取有效的电磁屏蔽措施。

2．中心机房组成

（1）中心机房组成应按计算机运行特点及设备具体要求确定，一般宜由主机房、基本工作间、第一类辅助房间、第二类辅助房间和第三类辅助房间等组成。

（2）中心机房的使用面积应根据网络与计算机设备的外形尺寸布置确定。在网络与计算机设备外形尺寸不完全掌握的情况下，各级网络与数据中心机房的使用面积应符合下列规定。

① 主机房面积可按下列方法确定。

当系统设备已选型时，可按下式计算

$$A = K\sum_{i=1}^{N} S_i$$

其中：A——主机房使用面积（单位为平方米）；

K——系数，取值为5～7；

S_i——第 i 个系统及辅助设备的投影面积（单位为平方米）；

N——机房内所有设备的总数。

当系统的设备尚未选型时，可按下式计算

$$A = KN$$

其中：N——机房内所有设备的总数；

K——单台设备占用面积，取值为4.5～5.5（单位为平方米/台）。

② 基本工作间和第一类辅助房间面积的总和，宜等于或大于主机房面积的 1.5 倍。

③ 硬件及软件人员办公室按每人 3.5～4m^2 计算。

3．设备布置

（1）网络与计算机设备宜采用分区布置，一般可分为服务器区、存储器区、网络设备区、安全设备区、通信区和监控区等。

（2）需要经常监视或操作的设备应布置于方便行走、便于操作的位置。

（3）产生尘埃及废物的设备应远离对尘埃敏感的设备，并宜集中布置在靠近机房的回风口处。

（4）主机房内通道与设备间的距离应符合下列规定。

① 两相对机柜正面之间的距离不应小于 1.5m。

② 机柜侧面（或不用面）距墙不应小于 0.5m，当需要维修测试时，则距墙不应小于 1.2m。

③ 走道净宽不应小于 1.2m。

2.6.2.2 环境条件

1. 温、湿度及空气含尘浓度

（1）主机房、基本工作间内的温、湿度必须满足网络与计算机设备的要求。

（2）机房内温、湿度应满足下列要求。

① 温度为20±2℃。

② 相对湿度为45%～65%。

③ 温度变化率<5℃/h 并不得结露。

（3）常用存储介质库的温、湿度应与主机房相同，特殊存储介质库的温、湿度应根据存储介质而定。

（4）主机房内的空气含尘浓度，在表态条件下测试，每升空气中大于或等于0.5μm的尘粒数，应少于18 000粒。

2. 噪声、电磁干扰、振动及静电

（1）主机房内的噪声，在计算机系统停机条件下，在主操作员位置测量应小于68dB。

（2）主机房内无线电干扰场强，在频率为0.15～1000MHz 时，不应大于126dB。

（3）主机房内磁场干扰环境场强不应大于800A/m。

（4）在计算机系统停机条件下，主机房地板表面垂直及水平方向的振动加速度值不应大于500mm/s^2。

（5）主机房地面及工作台面的静电泄漏电阻，应符合现行国家标准《计算机机房用活动地板技术条件》的规定。

（6）主机房内绝缘体的静电电位不应大于1kV。

3. 室内装饰

（1）主机房室内装饰应选用气密性好、不起尘、易清洁，并在温、湿度变化作用下变形小的材料，并应符合下列要求。

① 墙壁和顶棚表面应平整，减少积灰面，并应避免眩光。如为抹灰时，应符合高级抹灰的要求。

② 应铺设活动地板。活动地板应符合现行国家标准《计算机机房用活动地板技术条件》的要求。铺设高度应按实际需要确定，宜为 200～350mm。

③ 活动地板下的地面和四壁装饰可采用水泥砂浆抹灰。地面材料应平整、耐磨。当活动地板下的空间为静压箱时，四壁及地面均应选用不起尘、不易积灰、易于清洁的饰面材料。

④ 吊顶宜选用不起尘的吸声材料，如吊顶以上及作为铺设管线用时，其四壁应抹灰，楼板底面应清理干净；当吊顶以上空间为静压箱时，则顶部和四壁均应抹灰，并刷不易脱落的涂料。其管道的饰面也应选用不起尘的材料。

（2）基本工作间、第一类辅助房间的室内装饰应选用不起尘、易清洁的材料。墙壁和顶棚表面应平整，减少积灰面。装饰材料可根据需要采取防静电措施。地面材料应平整、耐磨、易除尘。

（3）主机房和基本工作间的内门、观察窗和管线穿墙等的接缝处，均应采取密封措施。

（4）中心机房室内色调应淡雅柔和。

（5）当主机房和基本工作间设有外窗时，宜采用双层金属密闭窗，并避免阳光的直射；当采用铝合金窗时，可采用单层密闭窗，但玻璃应为中空玻璃。

（6）当主机房内设有用水设备时，应采取有效的防止给排水漫溢和渗漏的措施。

4．噪声及振动控制

（1）主机房应远离噪声源，当不能避免时，应采取消声和隔声措施。

（2）主机房内不宜设置高噪声的空调设备。当必须设置时，应采取有效的隔声措施。

（3）当第二类辅助房间内有强烈振动的设备时，设备及其通往主机房的管道应采取隔振措施。

2.6.2.3　空气调节

1．一般规定

（1）主机房和基本工作间，均应设置空气调节系统。

（2）当主机房和其他房间的空调参数不同时，宜分别设置空调系统。

2．热湿负荷计算

（1）计算机和其他设备的散热量应按产品的技术数据进行计算。

（2）中心机房空调的热湿负荷应包括下列内容。

① 计算机和其他设备的散热。

② 建筑围护结构的传热。

③ 太阳辐射热。

④ 人体散热、散湿。

⑤ 照明装置散热。

⑥ 新风负荷。

3．气流组织

（1）主机房和基本工作间空调系统的气流组织，应根据设备对空调的要求、设备本身的冷却方式、设备布置密度、设备发热量以及房间温湿度、室内风速、防尘、消声等要求，并结合建筑条件综合考虑。

（2）气流组织形式应按计算机系统的要求确定。

（3）采用活动地板下送风时，出口风速不应大于3m/s，送风气流不应直对工作人员。

4．系统设计

（1）主机房要求空调的房间宜集中布置；室内温、湿度要求相近的房间宜相邻布置。

（2）主机房不宜设采暖散热器，如设散热器必须采取严格的防漏措施。

（3）主机房的风管及其他管道的保温和消声材料及其粘结剂，应选用非燃烧材料或难燃烧材料。冷表面需做隔气保温处理。采用活动地板下送风方式时，楼板应采取保温措施。

（4）风管不宜穿过防火墙和变形缝。如必须穿过时，应在穿过防火墙处设防火阀；穿过变形缝处，应在两侧设防火阀。防火阀应既可手动又能自控。穿过防火墙、变形缝的风管两侧各2m 范围内的风管保温材料，必须采用非燃烧材料。

（5）空调系统应设消声装置。

（6）主机房必须维持一定的正压。主机房与其他房间、走廊间的压差不应小于4.9Pa，与室外静压差不应小于9.8Pa。

（7）空调系统的新风量应取下列三种中的最大值。

① 室内总送风量的 5%。

② 按工作人员每人 $40m^3/h$。

③ 维持室内正压所需风量。

（8）主机房的空调送风系统，应设初效、中效两级空气过滤器，中效空气过滤器计数效率应大于80%，末级过滤装置宜设在正压端或送风口。

（9）主机房在冬季需送冷风时，可取室外新风作冷源。

（10）主机房空气调节控制装置应满足网络设备与电子计算机系统对温度、湿度等的要求。

5．设备选择

（1）空调设备的选用应符合运行可靠、经济和节能的原则。

（2）空调系统和设备选择应根据计算机类型、机房面积、发热量及对温、湿度和空气含尘浓度的要求综合考虑。

（3）空调冷冻设备宜采用带风冷凝器的空调机。当采用水冷机组时，对冷却水系统冬季应采取防冻措施。

（4）空调和制冷设备宜选用高效、低噪声、低振动的设备。

（5）空调制冷设备的制冷能力，应留有15%～20%的余量。

（6）设备长期连续运行，空调系统应有备用装置。

2.6.2.4 电气技术

1．供配电

（1）机房用电负荷等级及供电要求应按现行国家标准《供配电系统设计规范》的规

定执行。

（2）电子计算机供电电源质量要求如下。

① 稳态电压偏移范围（%）：±2。

② 稳态频率偏移范围（Hz）：±0.2。

③ 电压波形畸变率（%）：3～5。

④ 允许断电持续时间（ms）：0～4。

（3）机房供配电系统应考虑计算机系统有扩散、升级等可能性，并应预留备用容量。

（4）机房宜由专用电力变压器供电。

（5）机房内其他电力负荷不得由计算机主机电源和不间断电源系统供电，主机房内宜设置专用动力配电箱。

（6）采用表态交流不间断电源设备时，应按现行国家标准《供配电系统设计规范》和现行有关行业标准规定的要求，采取限制谐波分量措施。

（7）当城市电网电源质量不能满足电子计算机供电要求时，应根据具体情况采用相应的电源质量改善措施和隔离防护措施。

（8）机房低压配电系统应采用频率50Hz、电压220/380VTN-S 或 TN-C-S 系统。

（9）单相负荷应均匀地分配在三相线路上，并应使三相负荷不平衡度小于20%。

（10）电子计算机电源设备应靠近主机房设备。

（11）机房电源进线应按现行国家标准《建筑防雷设计规范》采取防雷措施。机房电源应采用地下电缆进线。当不得不采用架空进线时，在低压架空电源进线处或专用电力变压器低压配电母线处，应装设低压避雷器。

（12）主机房内应分别设置维修和测试用电源插座，两者应有明显区别标志。测试用电源插座应由计算机主机电源系统供电，其他房间内应适当设置维修用电源插座。

（13）主机房内活动地板下部的低压配电线路宜采用铜芯屏蔽导线或铜芯屏蔽电缆。

（14）活动地板下部的电源线应尽可能远离计算机信号线，并避免并排敷设；当不能避免时，应采取相应的屏蔽措施。

2．照明

（1）机房照明的照度标准应符合下列规定。

① 主机房的平均照度可按 200、300、500lx 取值。

② 基本工作间、第一类辅助房间的平均照度可按 100、150、200lx 取值。

③ 第二、三类辅助房间应按现行照明设计标准的规定取值。

（2）机房照度标准的取值应符合下列规定。

① 间歇运行的机房取低值。

② 持续运行的机房取中值。

③ 连续运行的机房取高值。

④ 无窗建筑的机房取中值或高值。

（3）工作区内一般照明的均匀度（最低照度与平均照度之比）不宜小于0.7，非工作区的照度不宜低于工作区平均照度的1/5。

（4）机房内应设置备用照明，其照度宜为一般照明的1/10。备用照明宜为一般照明的一部分。

（5）机房应设置疏散照明和安全出口标志灯，其照度不应低于0.51x。

（6）机房照明线路宜穿钢管暗敷或在吊顶内穿钢管明敷。

（7）大面积照明场所的灯具宜分区、分段设置开关。

（8）技术夹层内应设照明，采用单独支路或专用配电箱（盘）供电。

3．静电防护

（1）基本工作间不用活动地板时，可铺设导静电地面，导静电地面可采用导电胶与建筑地面粘牢，导静电地面的体积电阻率均应为1.0×107～1.0×1010Ω• cm，其导电性能应长期稳定，且不易发尘。

（2）主机房内采用的活动地板可由钢、铝或其他阻燃性材料制成。活动地板表面应是导静电的，严禁暴露金属部分。单元活动地板的系统电阻应符合现行国家标准《计算机机房用活动地板技术条件》的规定。

（3）主机房内的工作台面及坐椅垫套材料应是导静电的，其体积电阻率应为1.0×107～1.0×1010Ω• cm。

（4）主机房内的导体必须与大地作可靠的连接，不得有对地绝缘的孤立导体。

（5）导静电地面、活动地板、工作台面和坐椅垫套必须进行静电接地。

（6）静电接地的连接线应有足够的机械强度和化学稳定性。导静电地面和台面采用导电胶与接地导体粘接时，其接触面积不宜小于$10cm^2$。

（7）静电接地可以经限流电阻及自己的连接线与接地装置相连，限流电阻的阻值宜为1MΩ。

4．接地

（1）机房接地装置的设置应满足人身的安全及电子计算机正常运行和系统设备的安全要求。

（2）机房应采用下列 4 种接地方式。

① 交流工作接地，接地电阻不应大于 4Ω。

② 安全工作接地，接地电阻不应大于 4Ω。

③ 直流工作接地，接地电阻应按计算机系统具体要求确定。

④ 防雷接地，应按现行国家标准《建筑防雷设计规范》执行。

（3）交流工作接地、安全保护接地、直流工作接地和防雷接地这4种接地宜共用一组接地装置，其接地电阻按其中最小值确定。若防雷接地单独设置接地装置，其余三种接地宜共用一组接地装置，其接地电阻不应大于其中最小值，并应按现行国家标准《建筑防雷设计规范》要求采取防止反击措施。

（4）对直流工作接地有特殊要求需单独设置接地装置的网络设备与电子计算机系统，其接地电阻值及与其他接地装置的接地体之间的距离，应按计算机系统及有关规定的要求确定。

（5）网络设备与电子计算机系统的接地应采取单点接地并宜采取等电位措施。

（6）当多个网络设备与电子计算机系统共用一组接地装置时，宜将各网络设备与电子计算机系统分别采用接地线与接地体连接。

2.6.2.5　给水排水

1．一般规定

（1）与主机房无关的给排水管道不得穿过主机房。

（2）机房内的给排水管道应采用难燃烧材料保温。

2．系统和管材

（1）机房应根据设备、空调、生活和消防等对水质、水温、水压和水量的不同要求分别设置循环和直流给水系统。

（2）循环冷却水系统应按有关规范进行水质稳定计算，并采取有效的防蚀、防腐、防垢及杀菌措施。

（3）机房内的给排水管道必须有可靠的防渗漏措施，暗敷的给水管道宜用无缝钢管，管道连接宜用焊接。

（4）循环冷却水管可采用工程塑料管或镀锌钢管。

2.6.2.6　消防与安全

1．一般规定

（1）电子计算机主机房、基本工作间应设洁净气体灭火系统，并应按现行有关规范的要求执行。

（2）机房应设火灾自动报警系统，并应符合现行国家标准《火灾自动报警系统设计规范》的规定。

（3）报警系统和自动灭火系统应与空调、通风系统连锁。空调系统所采用的电加热器，应设置无风断电保护。

（4）机房的安全设计，除执行本章的规定外，尚应符合现行国家标准《计算站场地安全要求》的规定。

（5）电子计算机用于非常重要的场所，其机房在工程设计中必须采取相应的技术措施。

2．消防设施

（1）凡设置洁净气体灭火系统及火灾探测器的机房，其吊顶的上、下及活动地板下，均应设置探测器和喷嘴。

（2）主机房宜采用感烟探测器。当设有固定灭火系统时，应采用感烟、感温两种探测器的组合。

（3）当主机房内设置空调设备时，应受主机房内电源切断开关的控制。机房内的电源切断开关应靠近工作人员的操作位置或主要出入口。

3．安全设施

（1）主机房出口应设置向疏散方向开启且能自动关闭的门。并应保证在任何情况下都能从机房内打开。

（2）凡设有洁净气体灭火装置的机房，应配置专用的空气呼吸器或氧气呼吸器。

（3）机房内存放废弃物，应采用有防火盖的金属容器。

（4）机房内存放记录介质，应采用金属柜或其他能防火的容器。

（5）根据主机房的重要性，可设警卫室或保安设施。

（6）机房应有防鼠、防虫措施。

2.6.2.7 机房区域划分

机房应根据功能和设备类别实现区域划分，实现模块化一体管理，在统一规划的原则下充分满足网络发展的需要，达到方便维护，迅速响应，灵活扩充，保护投资的目的。

1．机房服务功能划分

根据机房所服务的对象和要实现的功能，对于无人值守的机房，在建设初期至少应规划中心服务器区、数据存储区、托管服务器区、核心网络区、线路设备区、安全系统区以及设备配线区 7 个区域。有人值守的机房在上述 7 个区域之外，还可以规划专门的管理区域，各区域规划应细化到以机柜为单位。

（1）中心服务器区。用于安装中心服务器，主要包括中心应用支撑平台所涉及的服务群和中心管理服务器群，以及中心所涉及的主要应用服务器和门户服务器群。

（2）数据存储区。用于安装中心数据存储设备，主要包含磁盘阵列、磁带库（机）、存储交换机和存储备份系统管理服务器等。

（3）托管服务器区。用于安装除中心服务器外的托管在机房的应用和托管主机，网络中各分支节点不具备机房条件和运行维护管理条件的，应将服务器托管于上级机房中。

（4）核心网络区。用于安装核心网络设备，是整个网络平台的汇结点，主要包含核心交换机（路由器）、城域网汇聚设备、服务器接入交换机、门户网络设备和 Internet 设备等。

机房建设单位应尽量独立划分该区域。如果涉及办公网络，接入网络设备不推荐安装在该区域中。

（5）线路设备区。用于安装线路传输设备，主要提供对长途线路的设备管理服务，应根据线路提供的服务商独立安排机柜。

（6）安全系统区。用于安装网络建设所涉及的相关安全设备，宜根据不同的安全防

护等级独立安排机柜。

机房建设初期至少应规划中心内部安全和外部安全两个设备柜。

（7）设备配线区。在机房设计时，建议采用集中配线方式，所有设备之间的连接线路，应在独立的配线柜中通过跳线方式完成。机房内应根据独立配线柜的建设要求，规划设备配线区。设备配线区用于安装机房内设备间跳线的配线架，主要提供对机房内的配线服务，应根据连接线的种类独立入柜，至少应包含光配和电配。其中，光配侧统一采用 ST 接头（设备侧统一采用 SC 接头），电配统一采用 RJ-45 接头。机房内设备间连接采用多模 850nm 光纤，远程连接采用 1310nm 光纤连接。

机房内部跨机柜连接线应桥架到集中配线架，通过集中配线架条线实现连接，实现机房内灵活调整，方便扩展和管理。

2．机房配套设施划分

为保证机房内设备安全稳定运行，在机房建设初期应建设强电配电区、不间断电源保障区、新风空调区以及消防设施区 4 种配套设施区域。

（1）强电配电区。用于机房内 220V 强电配电设备安装，宜在该区域地板上贴上黄色警告线，或在区域内设立显眼的标识牌。该区域应根据强电路数独立入柜，为中心机房提供可靠的电源保障系统，并且应与设备机柜间形成完整的防雷接地系统。

（2）不间断电源保障区（UPS 间）。建议与设备间采用建筑方式隔离，承重地板应根据 UPS 重量采取增加钢梁等手段加固。

（3）其他区域。包括新风空调区、消防设施区的设计，都应符合 GB 50174—1993 和前文所描述的要求。

2.6.2.8　机柜使用规范

1．服务器机柜设备部署

服务器机柜每机柜安装的服务器数目以 4～5 台为宜，配线架间隔 2U，托盘间隔 6U。机柜底部为统一的光配线架与电口配线架，连接至独立配线机柜。详细情况如图 2-83 所示。

2．网络机柜设备部署

网络机柜每机柜安装的网络设备，若大小为6～10U，则不宜超过2台；若大小为4U，则不宜超过4台；若大小为1U，则不宜超过8台。机柜底部为统一的光配线架与电口配线架，连接至独立配线机柜。详细情况如图2-84所示。

3．电口配线柜设备部署

电口配线柜应独立设置，其配线架与设备机柜的配线架通过双绞线互连。电口配线柜安装10个48口2U 配线架，间隔为1U，详细情况如图2-85所示。

4．光口配线柜设备部署

光口配线柜应独立设置，其配线架与设备机柜的配线架通过光纤互连。光口配线柜安装16个24芯1U 光配线架，间隔为1U，详细情况如图2-86所示。

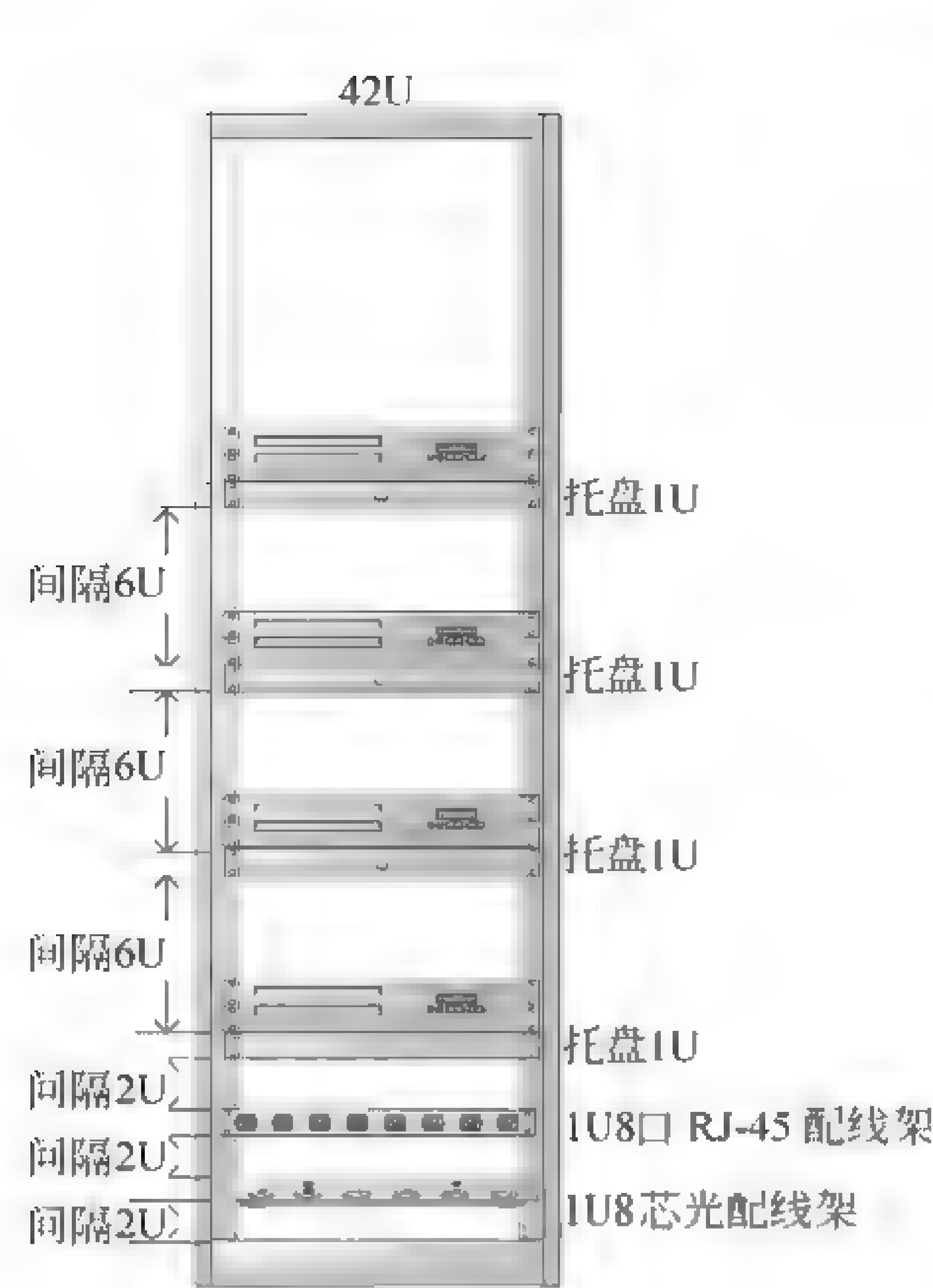


图 2-83 服务器机柜设备部署图

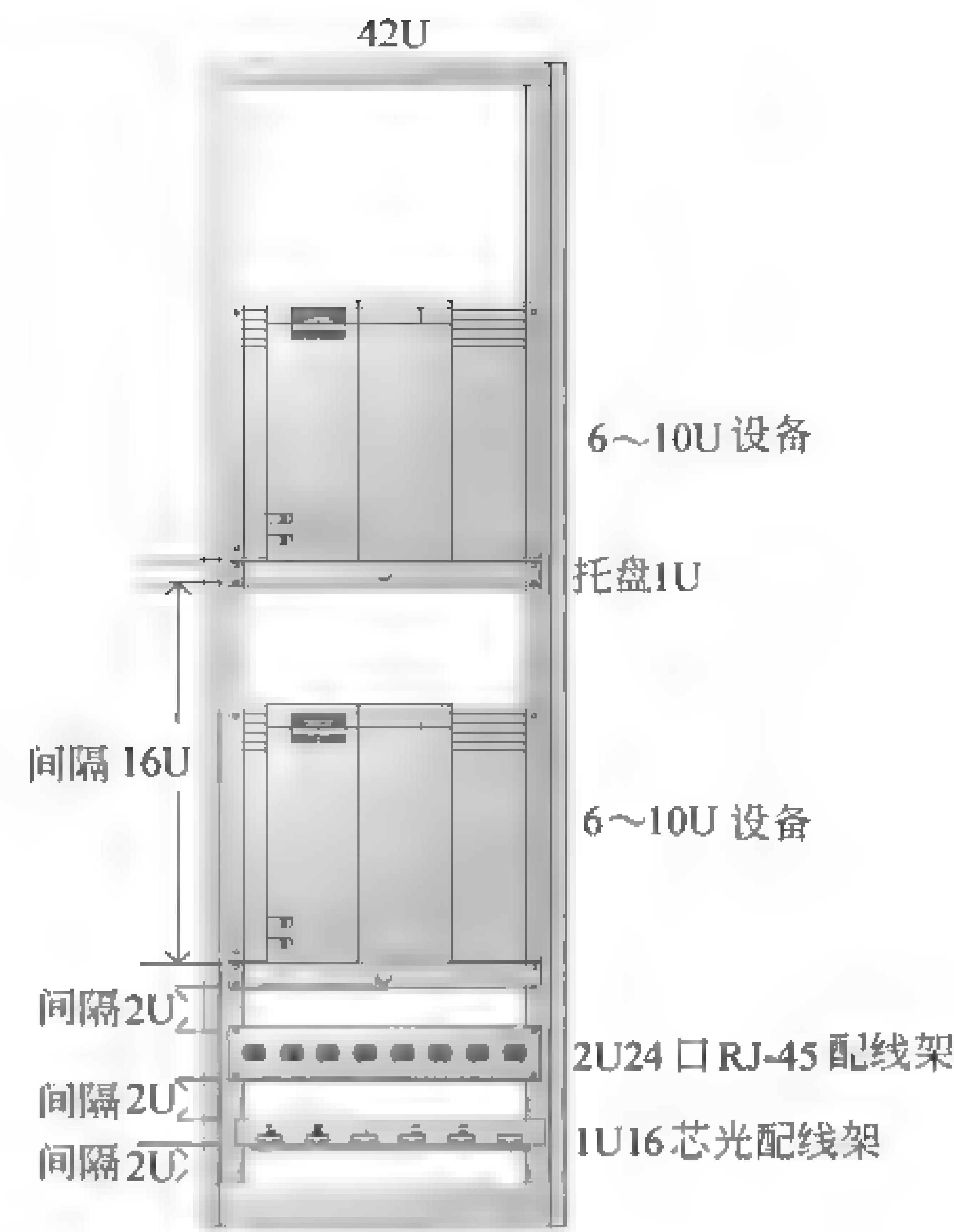


图 2-84 网络机柜设备部署图

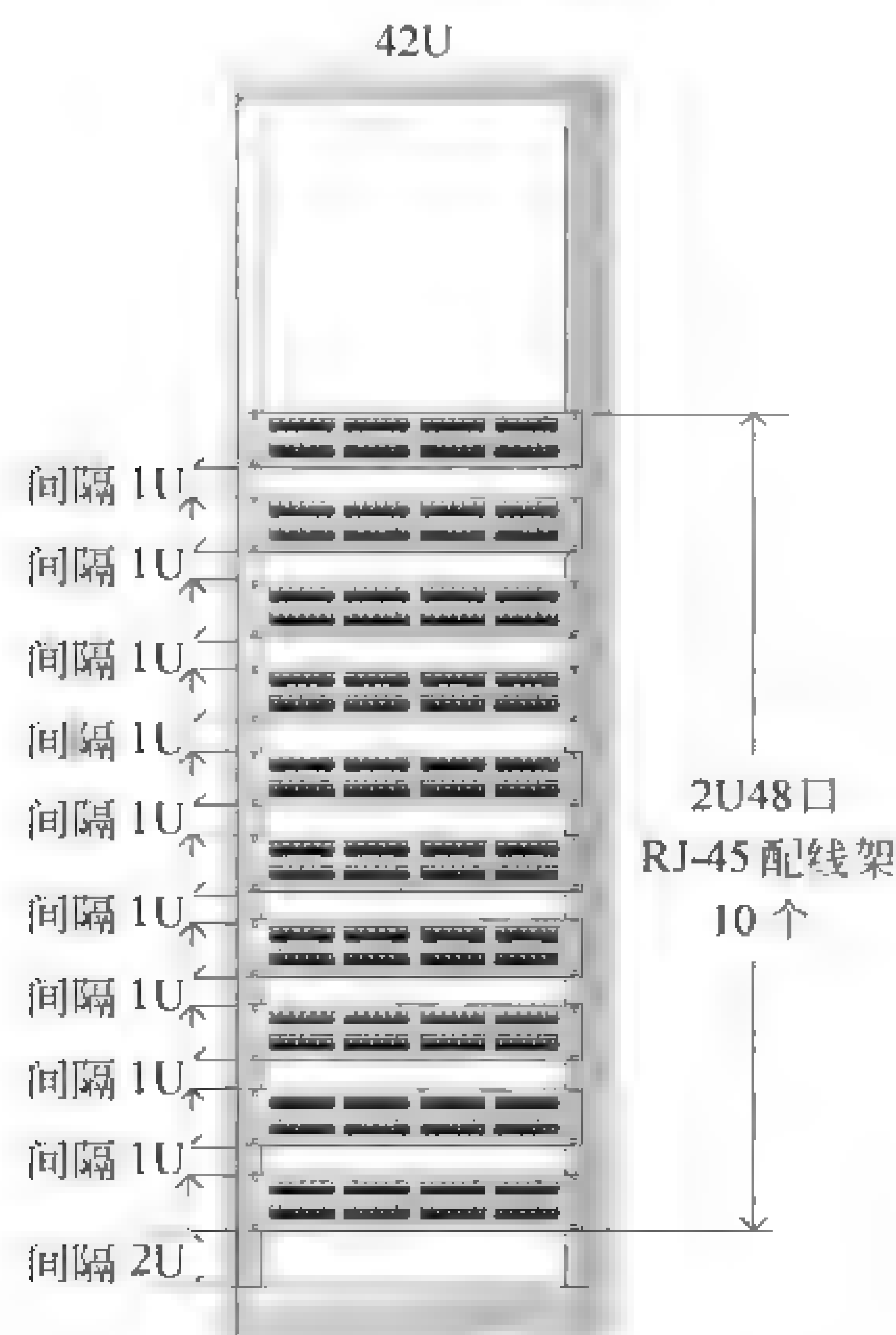


图 2-85 电口配线柜设备部署图

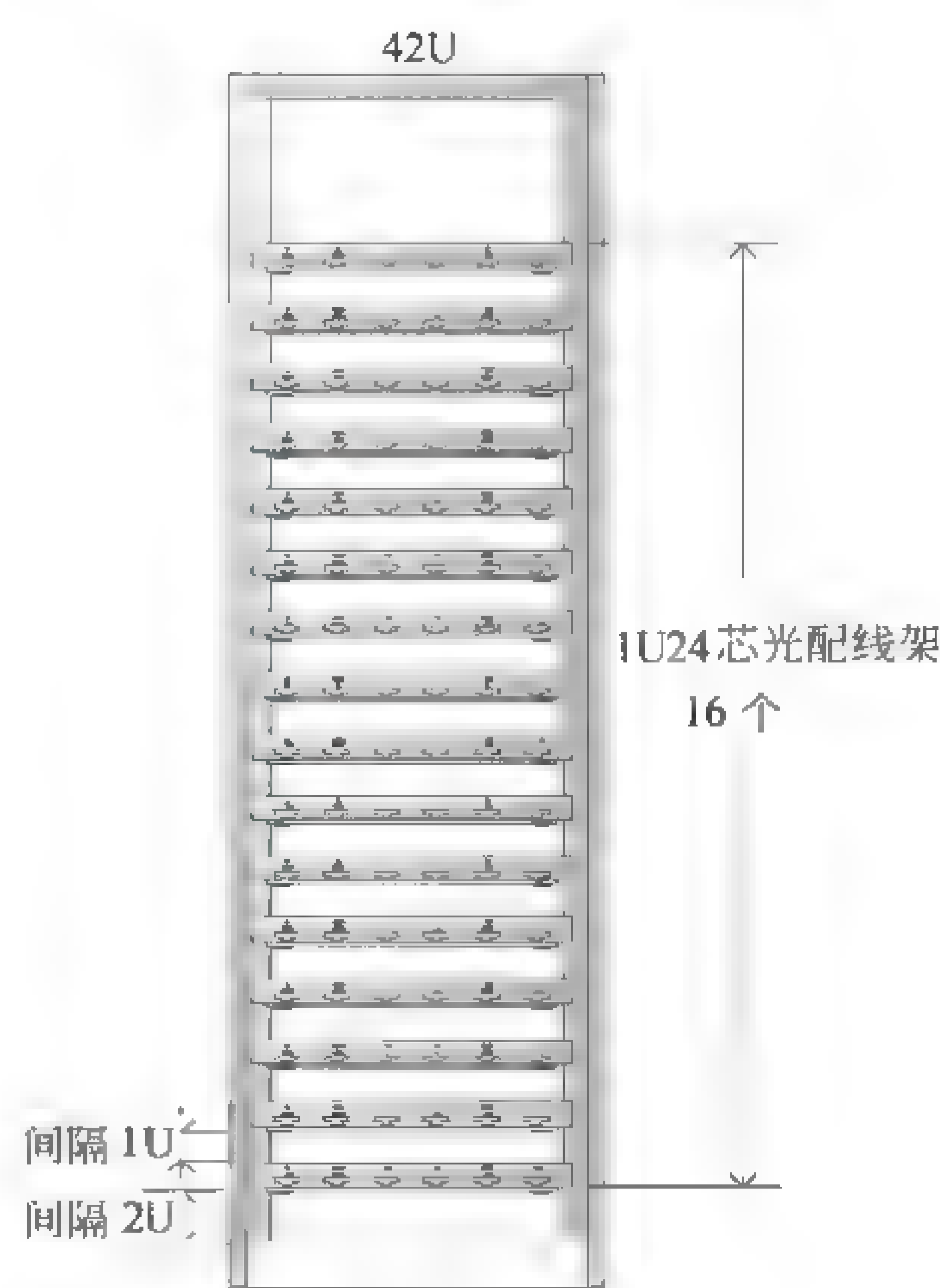


图 2-86 光口配线柜设备部署图

2.6.2.9　标签牌使用规范

1．机柜标签

机柜标签用于标识机柜功能区域和机柜编号，如图2-87所示。机柜标签应包含机柜功能区域名称、机柜编号，其中机柜编号前一个数字为排号，后一个数字为列号。标牌应采用金属或塑料材质，图中尺寸可根据设计者习惯进行调整。

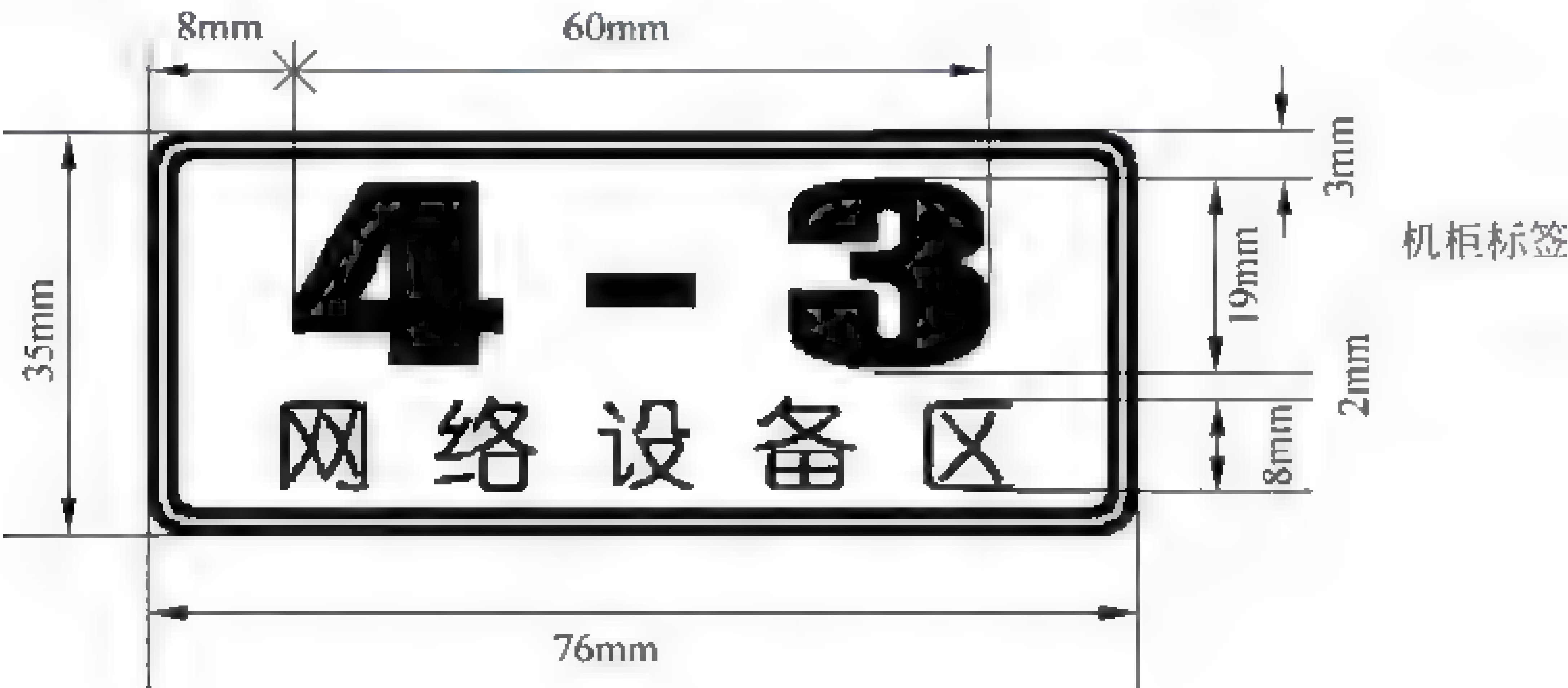


图 2-87　机柜标签

2．设备标签

设备标签用于标识机柜内设备，如图2-88所示。设备标签应至少包含设备型号、设备名称、管理地址、设备产地、投运日期、项目号、生产厂家、供货商和设备编号等信息，可适当添加其他信息，例如维护电话、厂商电话等。其中，设备编号为机柜内序列号（No.08表示从上至下第8台设备），图中的标牌尺寸可根据设计者习惯进行调整。



图 2-88　设备标签

3．线路标签

线路标签用于标识机房内线路，如图2-89所示。线路标签应至少包含线路类别、机柜号、设备号和端口号，详细尺寸可以根据需要进行调整。

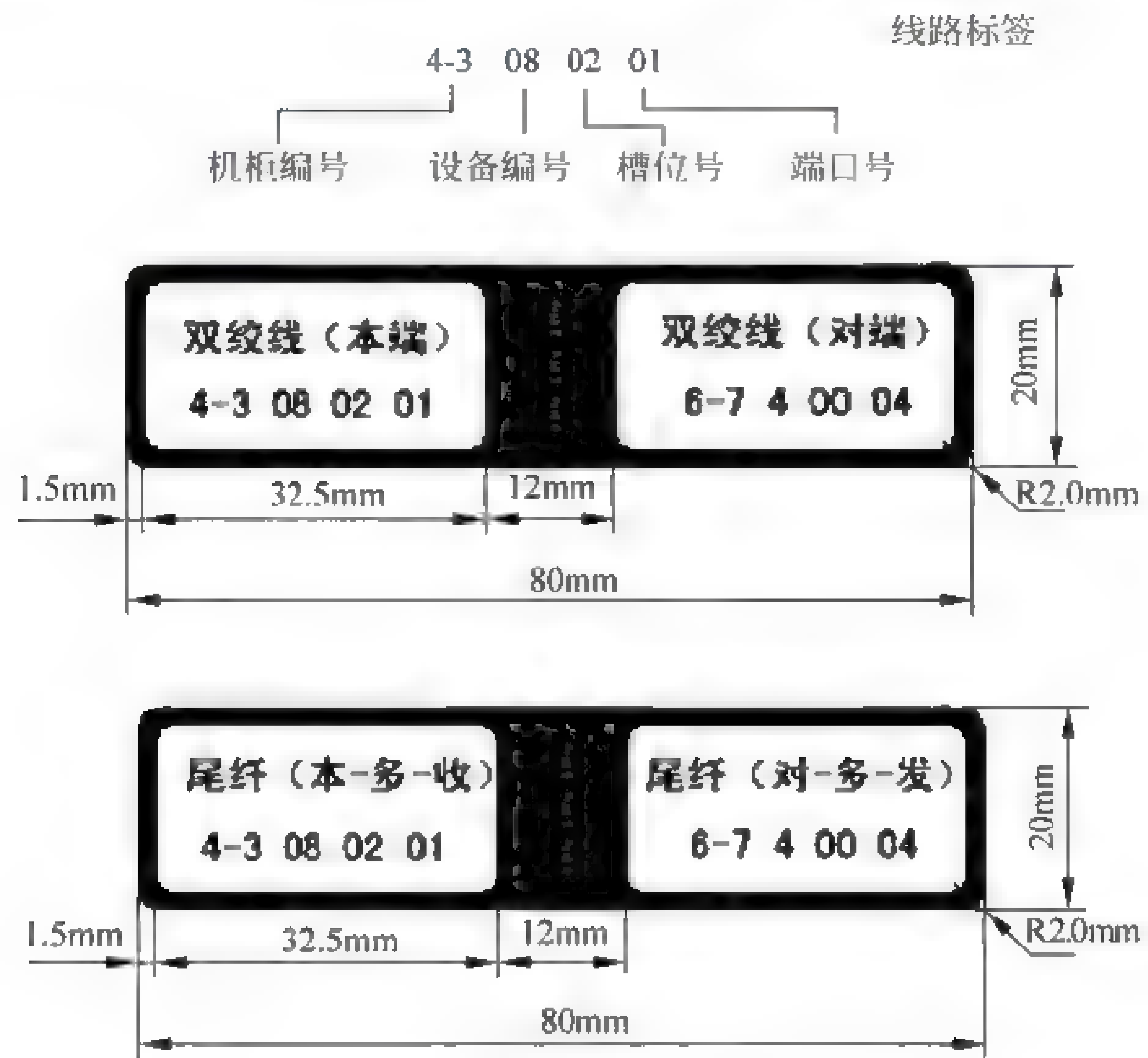


图 2-89 线路标签

4．设备名称编码规范对照表

与设备有关的所有文献资料等，都应采用统一的设备名称编码，设备名称编码规范对照表如表2-18所示。

表 2-18 设备名称编码规范对照表

设备名称编码规则						
应用	字段	第一字段	第二字段	第三字段	第四字段	第五字段
	说明	所属单位缩写	设备型号	设备分类	设备序号	区域缩写
固定资产管理文本档案	卡片编号	ZX	AR4640	N	0018	
	设备编号	ZX	AR4640	N	0018	
	技术资料编号	ZX	AR4640	N	0018	
设备软名	Sysname	ZX	AR4640	0018		S

续表

应用	字段	第一字段	第二字段	第三字段	第四字段	第五字段
	说明	所属单位缩写	设备型号	设备分类	设备序号	区域缩写
所属单位缩写：单位名中关键字拼音的第一个字母大写组合						
设备型号：被编码设备的具体型号						
设备分类：设备所属类别（参照设备分类缩写对照表）						
设备序号：顺序排序从0000到9999设备管理员分配						
区域缩写：网络划分的多个区域的缩写（参照区域缩写对照表）						
编码规则应用范围：固定资产管理，设备软名，文本档案						

设备分类缩写参考对照表

序号	分类	涵盖内容	英文名	缩写字段	备注
1	网络	路由器、交换机、拨号服务器、光纤收发器、防火墙、入侵检测	networks	N	
2	服务器	含小型机、工作站、PC 服务器	server	S	
3	个人计算机	含便携式计算机	computer	C	
4	外部设备	打印机、扫描仪、绘图仪等	peripheral equipment	P	
5	辅助设备	网络及服务器机柜、空调、UPS 等	assistant equipment	A	
6	工具	含网络工具、普通工具等	tools	T	
7	软件	系统软件、应用软件、数据库软件、工具软件	software	s	小写字母 s
8	其他		the others	t	小写字母 t
缩写字段为分类的英文名的第一个字母大写（软件和其他因为第一个字母和以上冲突因此采用小写加以区分）					

2.6.2.10　设计图纸

机房设计是物理设计中的关键内容，在实际工程项目中，应根据需要针对机房的不同建设内容分别形成设计图纸。通常情况下，需要独立成图的内容如下。

（1）室内装饰效果图。

（2）区域划分及隔断设计图。

（3）空调设计图。

（4）机房新风设计图。

（5）机房强电系统设计图。

（6）机房弱电系统设计图。

（7）机房照明系统设计图。

（8）机房静电及防雷设计图。
（9）机房给水排水设计图。
（10）机房防水设计图。
（11）机房消防设计图。
（12）机房防雷设计图。
（13）机房安防设计图。
（14）机房监控设计图。

2.6.3 设备选型

在物理网络设计阶段，根据需求说明书、通信规范说明书和逻辑网络设计说明书选择设备的品牌和型号的工作，是较为关键的任务之一。

在进行设备的品牌、型号的选择时，应该考虑到以下方面的内容。

1．产品技术指标

产品的技术指标是决定设备选型的关键，所有可以选择的产品，都必须满足依据通信规范分析中产生的技术指标，也必须满足逻辑网络设计中形成的逻辑功能。

利用通信规范说明书和逻辑网络设计说明书，可以形成网络设备的各项性能指标和功能要求，设计人员应对市场上的主流产品和型号进行过滤，将不满足要求的产品过滤掉，形成可供选择的品牌及型号集合。

后续的选型工作，就是依据多种约束条件在该集合中进行挑选。

2．成本因素

除了产品的技术指标之外，设计人员和用户最关心的就是成本因素，网络中各种设备的成本主要包括购置成本、安装成本和使用成本。

（1）购置成本。购置成本主要是指采购设备的投入，设计人员需要对不同品牌型号产品的市场通用价格进行比较，同时还要考虑批量采购的折扣、进口产品在特殊行业免税政策等因素。

（2）安装成本。安装成本包括运输成本、安装前的寄存成本、设备安装成本和调试成本等。对于普通网络设备或者设备数量较小的网络工程，这些成本可以不用考虑；但是对于大型网络项目，由于设备数量多、覆盖范围广，甚至还可能使用大型机等特殊设备，安装成本在整个成本因素中的比例较大，则不能忽略。

（3）使用成本。使用成本是使用设备过程中周期性产生的成本，例如设备维护、巡检和保养等。设计人员尤其要注意使用成本因素，过高的使用成本将导致设备很快就会被淘汰。

设计人员要针对不同品牌型号产品的成本进行估算，并形成相应的对照表，以便于用户进行选择。

3. 原有设备的兼容性

在产品选型过程中，与原有设备的兼容性是设计人员必须考虑的内容。

购置的网络设备必须与原有设备能够实现线路互连、协议互通，才能有效地利用现有资源实现网络投资的最优化。另外，保证与原有设备的兼容性，也降低了网络管理人员的管理工作量，利于实现全网统一管理。

如果一个网络中，大多数网络产品都是一个品牌，则新购置的产品采用相同的品牌是一个非常不错的选择，但是设计人员也必须考虑由于指定品牌而导致的厂商垄断价格、用户购置成本高等经常出现的情况。因此，大多数网络工程设计中，设计人员面对这种情况时，会将原有品牌作为首选产品，但是仍然会设计 2～3 种备用或兼容品牌，以形成一定的竞争关系。

4. 产品的延续性

产品的延续性是设计人员保证网络生命周期的关键因素，产品的延续性主要体现在厂商对某种型号的产品是否继续研发、继续生产、继续保证备品配件供应、继续提供技术服务。

在进行网络设备选型时，对于厂商已经明确表示不再进行投入或者在一至两年内即将停产的产品，是不能纳入可选择产品范围的。

5. 设备可管理性

设备可管理性是进行设备选型时的一个非关键因素，但也是必须考虑的内容。

设计人员在购置设备时，必须考虑设备的管理手段，以及是否能够纳入现有或规划的管理体系中。目前，大多数设备都是可以通过通用协议纳入管理平台的，同时也提供了标准的管理接口。在成本等方面的因素相同时，应尽可能选择采用通用管理协议、提供标准管理接口、能够纳入统一管理平台的产品。

6. 厂商的技术支持

对于大型网络工程中采用的大量设备，普通的网络管理人员只能完成日常的简单维护，对设备进行检测、保养和维修等工作必须借助于特定的专业人员。由于网络产品的特殊性，即使是部分网络集成商，也不能提供有效、合理的技术支持服务。对于这些设备的选择，就必须考虑厂商的技术支持。

厂商的技术支持一般包括定期巡检、电话咨询服务、现场故障排除和备品备件等，设计人员在选择产品时，可以比较不同品牌在本地的分支机构、服务人员数量、售后服务电话和技术支持价格等因素，为设备选型提供一定的依据。

7. 产品的备品备件库

产品的备品备件服务是厂商为了提供较为优质的服务，而形成的常备空闲设备、配件机制。通过在一个备品备件中心储备适量的设备或者配件，一旦该中心覆盖区域内用户产生设备或者配件故障，则可以从中心抽调备品备件进行临时替换，避免维修工作导致网络服务中断。

设计人员可以将备品备件库作为设备选型的一个参考因素，在其他条件相同的情况下，尽量选择本地或附近城市具有良好备品备件库的产品。对于一些不能中断服务的特殊网络，例如电力系统的生产调度网络来说，备品备件库的要求就不再是一个参考因素，而是一个决定性因素了。

8．综合满意度分析

在进行设备选型时，设计人员和用户会面对多种设备的选择，同时又会面临不同的选择角度，这些角度之间甚至是相互矛盾的。为了解决这种问题，可以采用综合满意度分析方法，该方法针对不同的角度制定特定的满意度评估标准，将每个角度的最高满意度定为 1。同时，根据设计人员、普通用户代表和网络管理部门负责人的协商，形成不同角度的比重权值，这些权值之和为 1。在进行设备选型时，组织有关人员和技术专家对待选的产品进行满意度评定，对多个评定结果计算平均值，将最终满意度最接近 1 的产品型号作为首选，并依据满意度的评定顺序依次产生候选产品。

2.6.4 物理网络设计文档

物理网络设计文档的作用是说明在什么样的特定物理位置实现逻辑网络设计方案中的相应内容，以及怎样有逻辑、有步骤地实现每一步的设计。此文档详细地说明了连接到网络设备的线缆的类型，以及网络中设备和连接器的布局，即线缆要经过什么地方，设备和连接器要安放的位置，以及它们是如何连接起来的。

物理网络设计文档的内容如下。

物理网络设计文档要清楚、简明，还必须正确和完整，包括以下要素。

（1）主管人员评价。

（2）物理网络设计图表。

（3）注释和说明。

（4）软硬件清单；

（5）最终费用估计。

（6）审批部分。

（7）物理网络设计的修改。

1．主管人员评价

相应主管人员需要对项目作简要概述，概述内容如下。

（1）简要地描述项目。

（2）列出设计过程各个阶段的内容。

（3）项目各个阶段的目前状态，包括已完成阶段和正在进行的阶段。

2．物理网络设计图表

物理网络设计图表给出的是一张详细的比例设计草图，是物理网络设计的结构蓝图。可以用它来估计所需线缆的数量，决定每部分线缆是否满足要求的长度等。由于物

理网络的实施都要使用这些图表，所以必须保证其正确性和清晰性。

3．注释和说明

为了帮助设计人员和非设计人员在较短的时间了解物理网络图，应该在图表中的相应位置加上说明和注释，用于具体说明设备连接的方式和安装的位置。这些注释应该说明所需线缆的类型、所遵循的布线方案、所考虑到的物理安全问题以及其他促使作出这些决定的依据。

4．软硬件清单

物理网络设计文档中除了物理网络图外，较为重要的一项就是详细描述网络实施所需的软硬件清单。列表清单内容如下。

（1）新的工具和零件。列出进行安装所需要的所有工具和零件，包括连接器、安装工具、软件以及书籍等。并把每个网络设备厂商的产品价格用表格的方式列出来。

（2）利用网络中现有的设备。如果部分或全部设备必须改装或升级，那么可以把相关材料源加到设备列表清单中。

（3）未应用的设备。对未应用的原有设备应该加以注释，说明这些设备是否可以用在其他网络的设计中，或者是否已经被淘汰。

5．最终费用估计

在物理设计完成以前，应该明确新建网络所需的硬件设备数量，然后使用先前已经得到审批的设计方案来进行招标，选择网络安装承包商，并估计人力费用和整个网络的安装费用。

6．审批部分

在物理设计方案实施前，必须通过高层人员的审批，并需要各个主管人员和网络设计组代表在物理设计文档说明书上签名。

7．物理网络设计的修改

物理网络设计是最接近施工的设计，设计方案的每一项改动都会直接影响到工程的实施。因此，必须有关于物理设计的修改约定，对可能产生变更的方面以及变更后的应对措施进行明确。

2.7　网络测试运行和维护

2.7.1　网络测试概述

1．网络测试现状

近年来随着网络规模扩大，网络带宽增加，异构性和复杂性不断提高，网络新业务不断出现，在这种情况下，网络运行质量的问题日益突出。网络运行质量好坏直接关系到网络能否正常运行及用户体验，因此在网络建设之初以及网络运行过程中有必要进行

网络测试。网络测试能获得第一手网络运行数据，为合理规划、建设网络，有效管理、维护网络奠定了基础。越来越多的技术和管理人员认识到网络测试的重要性，因为合理的网络测试是网络正常运行的基础，通过测试还能对网络日后的扩容提供参考数据，避免在网络建设、维护、使用方面的重复投资，这有利于降低管理成本、提高效益，同时通过测试能够加快网络部署的速度、迅速发现网络中的问题、确保网络中的各项服务。

2．网络测试方法

网络测试有多种测试方法，根据测试中是否向被测网络注入测试流量，可以将网络测试方法分为主动测试和被动测试。

主动测试是指利用测试工具有目的地主动向被测网络注入测试流量，并根据这些测试流量的传送情况来分析网络技术参数的测试方法。主动测试具备良好的灵活性，它能够根据测试环境明确控制测量中所产生的测量流量的特征，如特性、采样技术、时标频率、调度、包大小和类型（模拟各种应用）等。主动测试使测试能够按照测试者的意图进行，容易进行场景仿真。主动测试的问题在于安全性。主动测试主动向被测网络注入测试流量，是“入侵式”的测量，必然会带来一定的安全隐患。如果在测试中进行细致的测试规划，可以降低主动测试的安全隐患。

被动测试是指利用特定测试工具收集网络中活动的元素（包括路由器、交换机和服务器等设备）的特定信息，以这些信息作为参考，通过量化分析实现对网络性能、功能进行测量的方法。常用的被动测试方式包括通过 SNMP 协议读取相关 MIB 信息，通过 Sniffer、Ethereal 等专用数据包捕获分析工具进行测试。被动测试的优点是它的安全性。被动测试不会主动向被测网络注入测试流量，因此就不会存在注入 DDoS、网络欺骗等安全隐患。被动测试的缺点是不够灵活，局限性较大，而且因为是被动地收集信息，并不能按照测量者的意愿进行测试，会受到网络机构、测试工具等多方面的限制。

3．网络测试工具

网络测试工具主要有线缆测试仪、网络协议分析仪和网络测试仪。线缆测试仪用于检测线缆质量，可以直接判断线路的通断状况。网络协议分析仪多用于网络的被动测试，分析仪捕获网络上的数据包和数据帧，网络维护人员通过分析捕获的数据可以迅速检查网络问题。网络测试仪是专用的软硬件结合的测试设备，具有特殊的测试板卡和测试软件，这类设备多用于网络的主动测试，能对网络设备、网络系统以及网络应用进行综合测试，具备典型的三大功能：数据报捕获、负载产生和智能分析。网络测试仪多用于大型网络的测试。

2.7.2 线路与设备测试

1．线路测试

网络线路测试是基础测试。在这个过程中，跳线、插座和模块等网络系统中各个连接部件的实际物理特性都可以被了解，这样用户可以清楚地了解每根线缆是怎样被安装

以及是否被正确连接。

统计数据表明，50%以上的网络故障与布线有关。网络线路介质种类丰富，有单模光纤、多模光纤、双绞线和同轴电缆等，同时接口类型也众多，有 RJ45 头、BNC 头和 RS232 头等。这些介质有些特性我们用肉眼便可识别，如物理外形、长短大小等，有些就必须用仪器检测，如线路串扰、传输频率和信号衰减等。绝大多数符合 ANSI/TIA/EIA-568A/B 互连标准验证的测试仪都带有识别开路、短路、错对和分叉等线对故障的功能，这些常见故障很可能是在压接模块和打线过程中就出现了。通过测试可以尽早地排除故障，以提高网络运行质量。

双绞线和光纤是目前应用最广泛的通信介质。根据 EIA/TIA568B 布线标准、TSB-67 测试标准，合格的双绞线与光纤布线应满足表 2-19 所示的测试指标。

表 2-19　双绞线与光纤测试指标

双绞线合格指标	线缆长度	线路衰减	阻抗	近端串扰	环路电阻	线路延时
	<100m	<23.2dB	100±5Ω	>24dB	<40Ω	<1μs
光纤合格指标	500m，波长 1300nm			500m，波长 850nm		
	衰减<2.6dB			衰减<3.9dB		

2．网络设备测试

对网络设备如交换机、路由器和防火墙等进行性能测试，目的是了解设备完成各项功能时的性能情况。性能测试的参数包括吞吐量、时延、帧丢失率、背靠背数据帧处理能力、地址缓冲容量、地址学习速率和协议的一致性等。测试主要是验证设备是否符合各项规范的要求，确保网络设备互联时不会出现问题。

常用网络设备测试标准如下。

（1）交换机。网络系统中使用的交换机的端口密度、数据帧转发功能、数据帧过滤功能、数据帧转发及过滤的信息维护功能、运行维护功能、网络管理功能及性能指标应符合产品规格说明。也可参考 YD/T 1096—2001、YD/T 1097—2001 的规定。

（2）路由器。网络系统中使用的路由器设备的接口功能、通信协议功能、数据包转发功能、路由信息维护、管理控制功能、安全功能及性能指标应符合产品规格说明。也可参考 GB/T 18019—1999、GB/T 18020—1999 和 YD/T 1132—2001 的规定。

（3）防火墙。网络系统中若使用防火墙设备，则设备的用户数据保护功能、识别和鉴别功能、密码功能、安全审计功能及性能指标应符合产品规格说明。也可参考 GB/T 18019—1999、GB/T 18020—1999 和 YD/T 1132—2001 的规定。

2.7.3　网络系统测试

网络系统测试主要是网络是否为应用系统提供了稳定、高效的网络平台，如果网络系统不够稳定，网络应用就不可能快速稳定。对于常规的以太网进行系统测试，主要包

括系统连通性、链路传输速率、吞吐率、传输时延及链路层健康状况测试等基本功能测试。

1．系统连通性

所有联网的终端都必须按使用要求全部连通。

1）系统连通性测试方法

系统连通性测试结构示意图如图2-90所示。

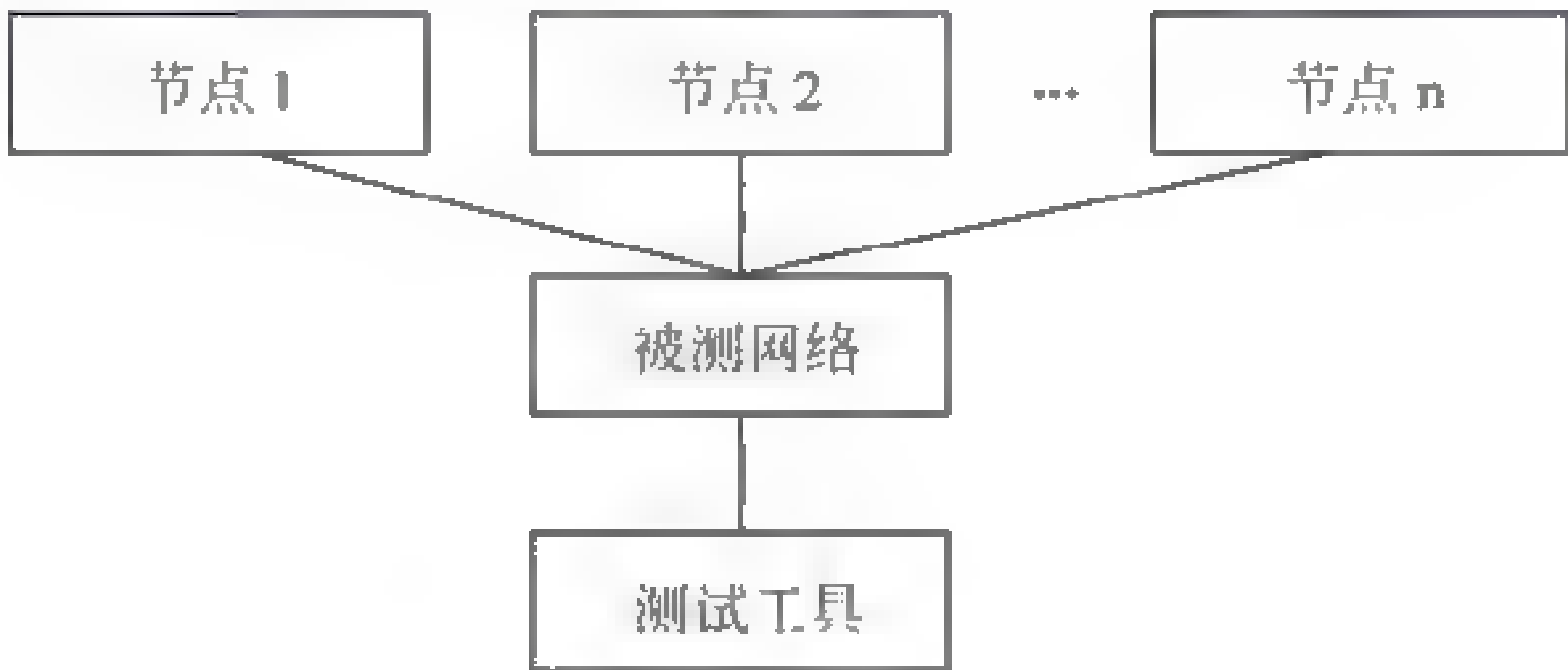


图 2-90 系统连通性测试结构示意图

（1）将测试工具连接到选定的接入层设备的端口，即测试点。

（2）用测试工具对网络的关键服务器、核心层和汇聚层的关键网络设备（如交换机和路由器）进行10次 Ping 测试，每次间隔1s，以测试网络连通性。测试路径要覆盖所有的子网和 VLAN。

（3）移动测试工具到其他位置的测试点，重复步骤（2），直到遍历所有测试抽样设备。

2）抽样规则

以不低于接入层设备总数 10%的比例进行抽样测试，抽样少于 10 台设备的，全部测试。每台抽样设备中至少选择一个端口，即测试点，测试点应能够覆盖不同的子网和 VLAN。

3）合格标准

（1）单项合格判据：测试点到关键节点的 Ping 测试连通性达到 100%时，则判定单点连通性符合要求。

（2）综合合格判据：所有测试点的连通性都达到 100%时，则判定系统的连通性符合要求；否则判定系统的连通性不符合要求。

2．链路传输速率

链路传输速率是指设备间通过网络传输数字信息的速率。对于 10M 以太网，单向最大传输速率应达到 10Mbps；对于 100M 以太网，单向最大传输速率应能达到 100Mbps；对于 1000M 以太网，单向最大传输速率应能达到 1000Mbps。发送端口和接收端口的利

用率关系应符合表 2-20 的规定。

表 2-20　发送端口和接收端口的利用率对应关系

网络类型	全双工交换式以太网		共享式以太网/半双工交换式以太网	
	发送端口利用率	接收端口利用率	发送端口利用率	接收端口利用率
10M 以太网	100%	≥99%	50%	≥45%
100M 以太网	100%	≥99%	50%	≥45%
1000M 以太网	100%	≥99%	50%	≥45%

1）链路传输速率测试方法



图 2-91　链路传输速率测试结构示意图

链路传输速率测试结构示意图如图 2-91 所示，测试工具 1 产生流量，测试工具 2 接收流量。若发送端口和接收端口位于同一机房，也可用一台具备双端口测试能力的测试工具实现。测试必须在空载网络中进行。

（1）将用于发送和接收的测试工具分别连接到被测网络链路的源和目的交换机端口或末端 HUB 端口上。

（2）对于交换机，测试工具1在发送端口产生100%满线速流量；对于 HUB，测试工具1在发送端口产生50%线速流量（建议将帧长度设置为1518字节）。

（3）测试工具2在接收端口对收到的流量进行统计，计算其端口利用率。

2）抽样规则

对核心层的骨干链路，应进行全部测试；对汇聚层到核心层的上联链路，应进行全部测试；对接入层到汇聚层的上联链路，以不低于 10%的比例进行抽样测试，抽样链路数不足 10 条时，按 10 条进行计算或者全部测试。

3）合格标准

发送端口和接收端口的利用率若符合表 2-20 的要求，则判定系统的传输速率符合要求，否则判定系统的传输速率不符合要求。

3．吞吐率

吞吐率是指空载网络在没有丢包的情况下，被测网络链路所能达到的最大数据包转发速率。

吞吐率测试需按照不同的帧长度（包括 64、128、256、512、1024、1280 和 1518 字节）分别进行测量。系统在不同帧大小情况下，从两个方向测得的最低吞吐率应符合表 2-21 的规定。

表 2-21　系统的吞吐率要求

测试帧长（字节）	10M 以太网		100M 以太网		1000M 以太网	
	帧/秒	吞吐率	帧/秒	吞吐率	帧/秒	吞吐率
64	≥14 731	99%	≥104 166	70%	≥1 041 667	70%
128	≥8361	99%	≥67 567	80%	≥633 446	75%
256	≥4483	99%	≥40 760	90%	≥362 318	80%
512	≥2326	99%	≥23 261	99%	≥199 718	85%
1024	≥ 1185	99%	≥11 853	99%	≥107 758	90%
1280	≥ 951	99%	≥9 519	99%	≥91 345	95%
1518	≥ 804	99%	≥8 046	99%	≥80 461	99%

1）网络吞吐率测试方法

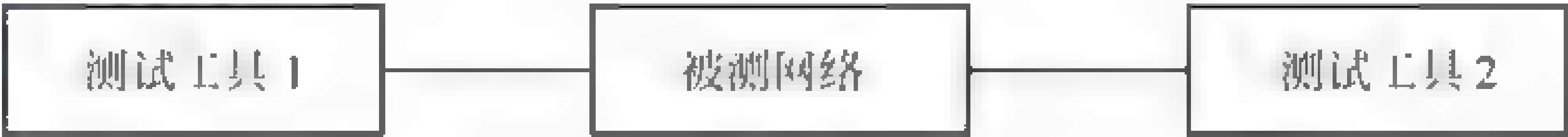


图 2-92　网络吞吐率测试结构示意图

网络吞吐率测试结构示意图如图 2-92 所示，测试工具 1 产生流量，测试工具 2 接收流量。若发送端口和接收端口位于同一机房，也可用一台具备双端口测试能力的测试工具实现。测试必须在空载网络下分段进行，包括接入层到汇聚层链路、汇聚层到核心层链路、核心层间骨干链路，以及经过接入层、汇聚层和核心层的用户到用户链路。

（1）将两台测试工具分别连接到被测网络链路的源和目的交换机端口上。

（2）先从测试工具1向测试工具2发送数据包。

（3）用测试工具1按照一定的帧速率，均匀地向被测网络发送一定数量的数据包。

（4）如果所有的数据包都被测试工具2正确接收到，则增加发送的帧速率；否则减少发送的帧速率。

（5）重复步骤（3），直到测出被测网络/设备在未丢包的情况下，能够处理的最大帧速率。

（6）分别按照不同的帧大小（包括64、128、256、512、1024、1280和1518字节）重复步骤（2）～（4）。

（7）从测试工具2向测试工具1发送数据包，重复步骤（3）～（6）。

2）抽样规则

对核心层的骨干链路，应进行全部测试；对汇聚层到核心层的上联链路，应进行全部测试；对接入层到汇聚层的上联链路，以不低于 10%的比例进行抽样测试，抽样链路数不足 10 条时，按 10 条进行计算或者全部测试；对于端到端的链路（即经过接入层、汇聚层和核心层的用户到用户的网络路径），以不低于终端用户数量 5%的比例进行抽

测，抽样链路数不足 10 条时，按 10 条进行计算或者全部测试。

3）合格标准

若系统在不同帧大小情况下，从两个方向测得的最低吞吐率值都符合表 2-21 的要求时，判定系统的吞吐率符合要求，否则判定系统的吞吐率不符合要求。

4．传输时延

传输时延是指数据包从发送端口（地址）到目的端口（地址）所需经历的时间。通常传输时延与传输距离、经过的设备和信道的利用率有关。在网络正常情况下，传输时延应不影响各种业务（如视频点播、基于 IP 的语音/VoIP 和高速上网等）的使用。

考虑到发送端测试工具和接收端测试工具实现精确时钟同步的复杂性，传输时延一般通过环回方式进行测量，单向传输时延为往返时延除以 2。系统在 1518 字节帧长情况下，从两个方向测得的最大传输时延应不超过 1 ms。

1）传输时延测试方法

当被测网络的收发端口位于不同的地理位置，测试结构示意图如图 2-93 所示，需要由两台工具来完成测试，测试工具 1 产生流量，测试工具 2 接收流量，并将测试数据流环回。当被测网络的收发端口位于同一机房，测试结构示意图如图 2-94 所示，可由一台具有双端口测试能力的测试工具完成，测试工具的一个端口用于产生流量，另一个端口用于接收流量。测试必须在空载网络下分段进行，包括接入层到汇聚层链路、汇聚层到核心层链路，以核心层间骨干链路，以及经过接入层、汇聚层和核心层的用户到用户链路。

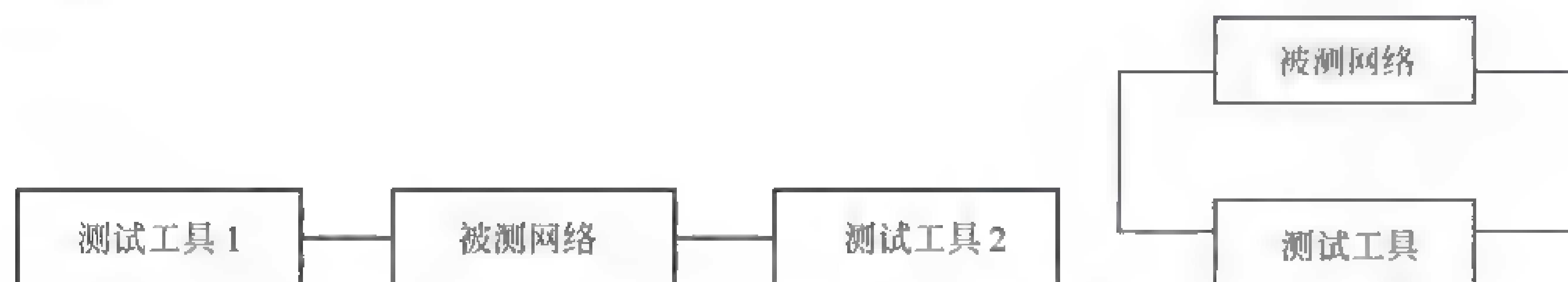


图 2-93　网络传输时延测试结构示意图（1）　　图 2-94　网络传输时延测试结构示意图（2）

（1）将测试工具（端口）分别连接到被测网络链路的源和目的交换机端口上。

（2）先从测试工具1（发送端口）向测试工具2（接口端口）均匀地发送数据包。

（3）向被测网络发送一定数目的1518字节的数据帧，使网络达到所测得的最大吞吐率。

（4）在图2-93中，由测试工具1向被测网络发送特定的测试帧，在数据帧的发送和接收时刻都打上相应的时间标记（Timestamp），测试工具2接收到测试帧后，将其返回给测试工具1。在图2-94中，测试工具通过发送端口发出带有时间标记的测试帧，在接收端口接收测试帧。

（5）测试工具1计算发送和接收的时间标记之差，便可得一次结果。

（6）重复步骤（3）～（4）20次，传输时延是对20次测试结果的平均值。

（7）在图2-93中，从测试工具2向测试工具1发送数据包，重复步骤（3）～（6），所得到时延是双向往返时延，单向时延可通过除2计算获得。在图2-94中，交换收发端口，重复步骤（3）～（6），所得到时延是单向时延。

2）抽样规则

对核心层的骨干链路，应进行全部测试；对汇聚层到核心层的上联链路，应进行全部测试；对接入层到汇聚层的上联链路，以不低于10%的比例进行抽样测试，抽样链路数不足10条时，按10条进行计算或者全部测试；对于端到端的链路（即经过接入层、会聚层和骨干层的用户到用户的网络路径），以不低于终端用户数量 5%的比例进行抽测，抽样链路数不足10条时，按10条进行计算或者全部测试。

3）合格标准

若系统在1518字节帧长情况下，从两个方向测得的最大传输时延都小于等于1 ms，则判定系统的传输时延符合要求，否则判定系统的传输时延不符合要求。

5．丢包率

丢包率是指网络在70%流量负荷情况下，由于网络性能问题造成部分数据包无法被转发的比例。在进行丢包率测试时，需按照不同的帧长度（包括64、128、256、512、1024、1280、1518字节）分别进行测量，测得的丢包率应符合表2-22的规定。

表2-22 丢包率要求

测试帧长（字节）	10M以太网		100M以太网		1000M以太网	
	流量负荷	丢包率	流量负荷	丢包率	流量负荷	丢包率
64	70%	≤0.1%	70%	≤0.1%	70%	≤0.1%
128	70%	≤0.1%	70%	≤0.1%	70%	≤0.1%
256	70%	≤0.1%	70%	≤0.1%	70%	≤0.1%
512	70%	≤0.1%	70%	≤0.1%	70%	≤0.1%
1024	70%	≤0.1%	70%	≤0.1%	70%	≤0.1%
1280	70%	≤0.1%	70%	≤0.1%	70%	≤0.1%
1518	70%	≤0.1%	70%	≤0.1%	70%	≤0.1%

1）丢包率测试方法

测试工具1 —— 被测网络 —— 测试工具2

图2-95 丢包率测试结构示意图

丢包率测试结构示意图如图2-95所示，测试工具1产生流量，测试工具2接收流量。若发送端口和接收端口位于同一机房，也可用一台具备双端口测试能力的测试工具实现。

测试链路应分段进行，包括接入层到汇聚层链路、汇聚层到核心层链路、核心层间骨干链路，以及经过接入层、汇聚层和核心层的用户到用户链路。

（1）将两台测试工具分别连接到被测网络链路的源和目的交换机端口上。

（2）测试工具1按一定的流量负荷，均匀地向被测网络发送一定数目的数据帧，测试工具2接收负荷，测试数据帧丢失的比例。

（3）发送的流量负荷从100%至10%以10%的步长依次递减，如果测得在某一流量负荷情况下丢包率为0%，则记录此时流量负荷。

（4）分别按照不同的帧大小（包括64、128、256、512、1024、1280和1518字节）重复步骤（3）。

2）抽样规则

对核心层的骨干链路，应进行全部测试；对汇聚层到核心层的上联链路，应进行全部测试；对接入层到汇聚层的上联链路，以不低于 10%的比例进行抽样测试，抽样链路数不足 10 条时，按 10 条进行计算或者全部测试；对于端到端的链路（即经过接入层、汇聚层和骨干层的用户到用户的网络路径），以不低于终端用户数量 5%的比例进行抽测，抽样链路数不足 10 条时，按 10 条进行计算或者全部测试。

3）合格标准

若系统在不同帧大小情况下测得的丢包率都符合表 2-22 的要求，则判定系统丢包率符合要求，否则判定系统丢包率不符合要求。

6. 以太网链路层健康状况指标

（1）链路利用率。链路利用率是指网络链路上实际传送的数据吞吐率与该链路所能支持的最大物理带宽之比。也可理解为网络从事传输数据时间与网络运行时间之比。

链路的利用率包括最大利用率和平均利用率。最大利用率的值同测试统计采样间隔有一定的关系，采样间隔越短，则越能反映出网络流量的突发特性，因此最大利用率的值就越大。对于共享式以太网和交换式以太网，链路的持续平均利用率应符合表 2-23 的规定。

（2）错误率及各类错误。错误率是指网络中所产生的各类错误帧占总数据帧的比率。常见的以太网错误类型包括长帧、短帧、有 FCS 错误的帧、超长错误帧、欠长帧和帧对齐差错帧，网络的错误率（不包括冲突）应符合表 2-23 的规定。

（3）广播帧和组播帧。在以太网中，广播帧和组播帧数量应符合表 2-23 的要求。

（4）冲突（碰撞）率。处于同一网段的两个站点如果同时发送以太网数据帧，就会产生冲突。冲突帧是指在数据帧到达目的站点之前与其他数据帧相碰撞，而造成其内容被破坏的帧。共享式以太网和半双工交换式以太网传输模式下，冲突现象是极为普遍的。过多的冲突会造成网络传输效率的严重下降。

冲突帧同发送的总帧数之比，称为冲突（或碰撞）率。一般情况下，网络的碰撞率应符合表 2-23 的规定。

表 2-23 链路的健康状况指标要求

测 试 指 标	技 术 要 求	
	共享式以太网/半双工交换式以太网	全双工交换式以太网
链路平均利用率（带宽%）	≤40	≤70
广播率（帧/秒）	≤50	≤50
组播率（帧/秒）	≤40	≤40
错误率（占总帧数%）	≤1	≤1
冲突（碰撞）率（占总帧数%）	≤5	0

2.7.4 网络应用测试

网络系统应用的性能测试是为确保网络在实际运行状况下，各种基本应用服务能够达到用户可以接受的性能和服务质量。

网络系统的基本应用服务主要包括 DHCP 服务、DNS 服务、Web 访问服务、E-mail 服务和文件服务。

1. 应用服务标准

（1）DHCP 服务性能指标。DHCP 服务器响应时间应不大于 0.5s。

（2）DNS 服务性能指标。DNS 服务器响应时间应不大于 0.5s。

（3）Web 访问服务性能指标。Web 访问服务器性能测试如下。

- HTTP 第一响应时间：内部网站点访问时间应不大于 1s。
- HTTP 接收速率：内部网站点访问速率应不小于 10000bps。

（4）E-mail 服务性能指标。E-mail 服务器主要指 SMTP 服务器和 POP3 服务器，其性能测试如下。

- 邮件写入时间：1K 字节邮件写入服务器时间应不大于 1s。
- 邮件读取时间：从服务器读取 1K 字节邮件的时间应不大于 1s。

（5）文件服务性能指标。文件服务器性能指标应符合表 2-24 的规定。

表 2-24 文件服务器性能指标要求

测 试 指 标	指标要求（文件大小为100KB）
服务器连接时间（s）	≤0.5
写入速率（bps）	>10 000
读取速率（bps）	> 10 000
删除时间（s）	≤0.5
断开时间（s）	≤0.5

2. 应用服务性能测试方法

应用服务性能测试结构示意图如图 2-96 所示。

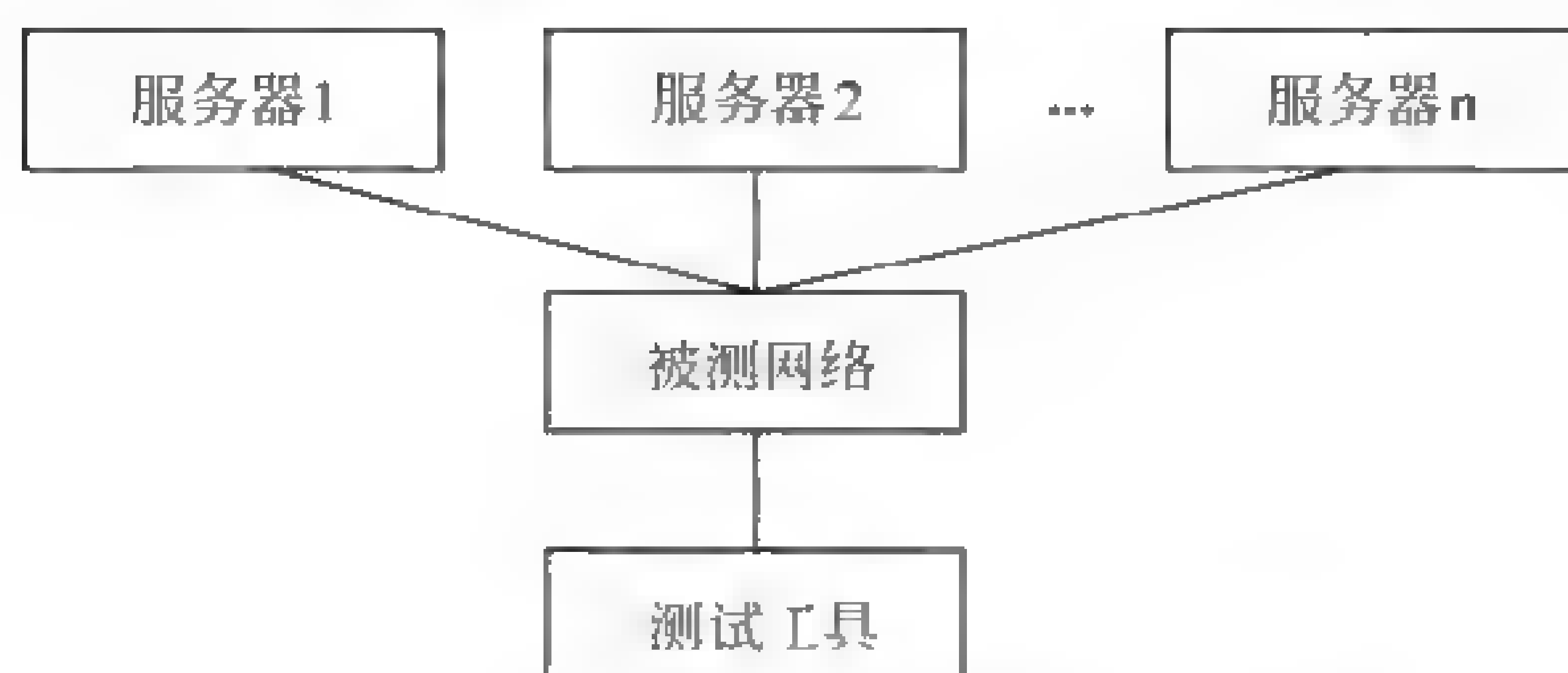


图 2-96　应用服务性能测试结构示意图

（1）将测试工具连接到被测网络的某一用户接入端口（网段）。

（2）用测试工具仿真终端用户，模拟一个用户访问被测服务器的全过程。对访问过程中各阶段性能指标进行测试，包括服务器响应时间、写入速率、读取速率、删除时间和断开时间等。

（3）重复步骤（2），对下一个服务器进行测试，直到测完所有的服务器。

（4）按照一定的时间间隔，重复步骤（2）～（3），共进行10次测试，记录10次测试结果的平均值。

（5）移动测试工具到其他网段，重复步骤（2）～（3），从而测试网络不同接入位置访问服务的性能水平。

测试点符合某应用服务要求时，判定该服务性能符合要求，否则判定该服务性能不符合要求。

2.7.5　测试报告

测试完成后最终应提供一份完整的测试报告，测试报告应对这次测试中的测试对象、测试工具、测试环境、测试内容和测试结果等进行详细论述。测试报告是整个网络工程文档的重要组成部分，人们对工程的满意程度和对工程质量的认可程度很大程度上来源于这份报告。

测试报告的形式并不固定，可以是一个简短的总结，也可以是很长的书面文档。通常测试报告包含以下信息。

（1）测试目的：用一两句话解释本次测试的目的。

（2）结论：从测试中得到的信息和推荐下一步的行动。

（3）测试结果总结：对测试进行总结并由此得出结论。

（4）测试内容和方法：简单地描述测试是怎样进行的，应该包括负载模式、测试脚本和数据收集方法，并且要解释采取的测试方法怎样保证测试结果和测试目的相关，测试结果是否可重现。

（5）测试配置：网络测试配置用图形表示出来。

测试报告包括对各测试项目的测试结果，应以数字、图形和列表等方式记录下来，结论则以书面文档方式叙述。完整、客观的测试报告是网络运行与维护的重要参考。

2.8 网络故障分析与处理

网络环境越复杂，发生故障的可能性就越大，引发故障的原因也就越难确定。网络故障往往具有特定的故障现象。这些现象可能比较笼统，也可能比较特殊。利用特定的故障排除工具及技巧，在具体的网络环境下观察故障现象，细致分析，最终必然可以查找出一个或多个引发故障的原因。一旦能够确定引发故障的根源，那么故障都可以通过一系列的步骤得到有效的处理。

2.8.1 网络故障排除思路

在排除网络中出现的故障时，使用非系统化的方法进行故障排除，可能会浪费大量宝贵的时间及资源，事倍功半，使用系统化的方法往往更为有效。系统化的方法流程如下：定义特定的故障现象，根据特定现象推断出可能发生故障的所有潜在的问题，直到故障现象不在出现为止。

图 2-97 给出了一性般故障排除模型的处理流程。这一流程并不是解决网络故障时必须严格遵守的步骤，只是为建立特定网络环境中故障排除的流程提供了基础。

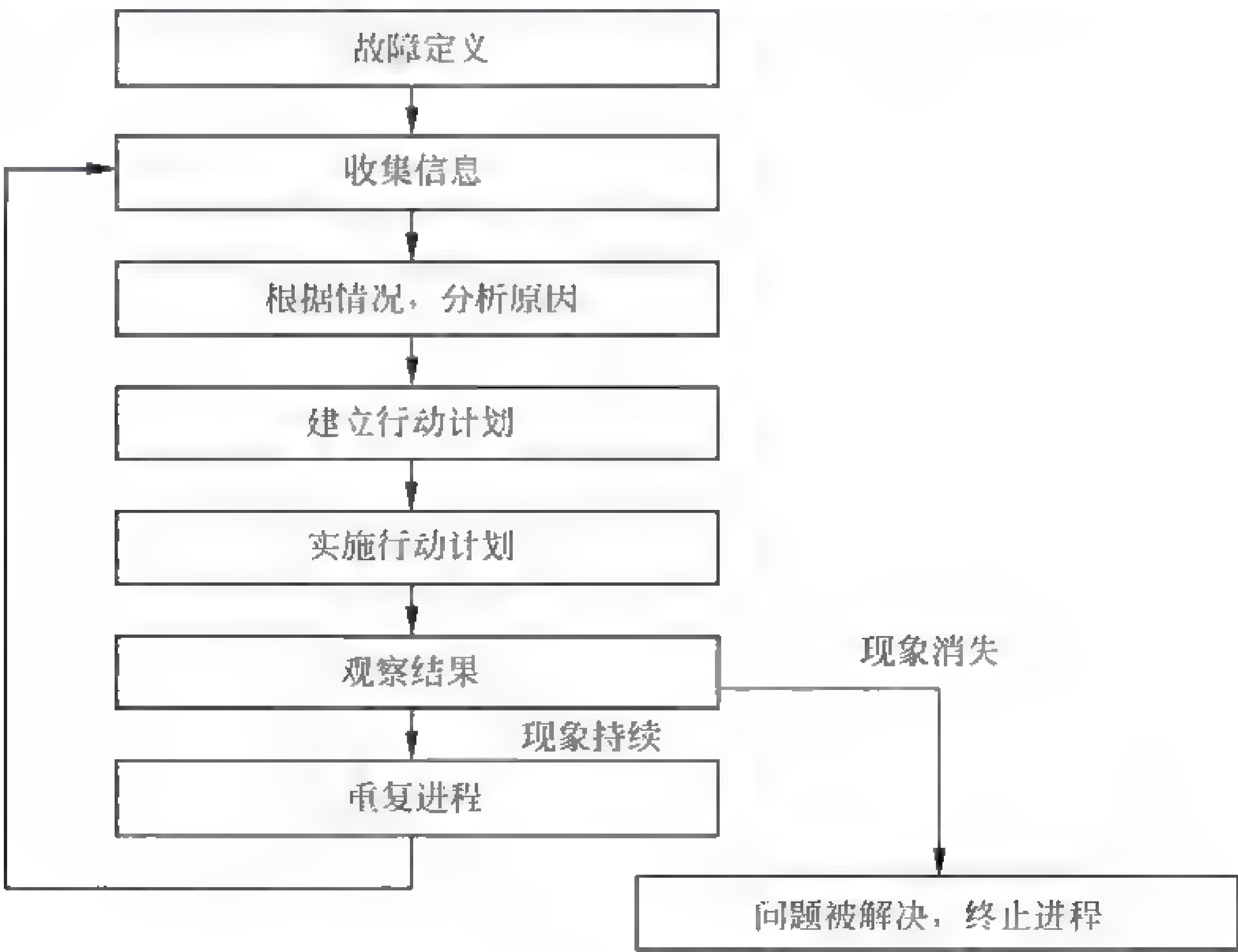


图 2-97 一般性故障排除模型

（1）分析网络故障时，要对网络故障有个清晰的描述，并根据故障的一系列现象以及潜在的症结对其进行准确的定义。

要想对网络故障做出准确的分析，首先应该了解故障表现出来的各种现象，然后确定可能会产生这些现象的故障根源或现象。例如，主机没有对客户机的服务请求做出响应（一种故障现象），可能产生这一现象的原因主要包括主机配置错误、网络接口卡损坏或路由器配置不正确等。

（2）收集有助于确定故障症结的各种信息。

向受故障影响的用户、网络管理员、经理及其他关键人员询问详细的情况。从网络管理系统、协议分析仪的跟踪记录、路由器诊断命令的输出信息以及软件发行注释信息等信息源中收集有用的信息。

（3）依据所收集到的各种信息考虑可能引发故障的症结。利用所收集到的这些信息可以排除一些可能引发故障的原因。

例如，根据收集到的信息也许可以排除硬件出现问题的可能性，于是就可以把关注的焦点放在软件问题上。应该充分地利用每一条有用的信息，尽可能地缩小目标范围，从而制定出高效的故障排除方法。

（4）根据剩余的潜在症结制订故障的排查计划。从最有可能的症结入手，每次只做一处改动。

之所以每次只做一处改动，是因为这样有助于确定针对固定故障的排除方法。如果同时做了两处或多处改动，也许能排除故障，但是难以确定到底是哪些改动消除了故障现象，而且对日后解决同样的故障也没有太大的帮助。

（5）实施制订好的故障排除计划，认真执行每一步骤，同时进行测试，查看相应的现象是否消失。

（6）当做出一处改动时，要注意收集相应操作的反馈信息。通常，应该采用在步骤（2）中使用的方法（利用诊断工具并与相关人员密切配合）进行信息的收集工作。

（7）分析相应操作的结果，并确定故障是否已被排除。如果故障已被排除，那么整个流程到此结束。

（8）如果故障依然存在，就得针对剩余的潜在症结中最可能的一个制订相应的故障排除计划。回到步骤（4），依旧每次只做一处改动，重复此过程，直到故障被排除为止。

如果能提前为网络故障做好准备工作，那么网络故障的排除也就变得比较容易了。对于各种网络环境来说，最为重要的是保证网络维护人员总能够获得有关网络当前情况的准确信息。只有利用完整、准确的信息才能够对网络的变动做出明智的决策，才能够尽快、尽可能简单地排除故障。因此，在网络故障的排除过程中，最为关键的是确保当前掌握的信息及资料是最新的。

对于每个已经解决的问题，一定要记录其故障现象以及相应的解决方案。这样，就可以建立一个问题/回答数据库，今后发生类似的情况时，公司里的其他人员也能参考这

些案例。从而极大地降低对网络进行故障排除的时间，最小化对业务的负面影响。

2.8.2 网络故障排除工具

排除网络故障的常用工具有多种，总的来说可以分为三类：设备或系统诊断命令、网络管理工具以及专用故障排除工具。

1．设备或系统诊断命令

许多网络设备及系统本身就提供大量的集成命令来帮助监视并对网络进行故障排除。下面介绍了一些常用命令的基本用法。

- show 命令：可以用于监测系统的安装情况与网络的正常运行状况，也可以用于对故障区域的定位。
- debug 命令：帮助分离协议和配置问题。
- ping 命令：用于检测网络上不同设备之间的连通性。
- trace 命令：可以用于确定数据包在从一个设备到另一个设备直至目的地的过程中所经过的路径。

1）show

show 命令是一个功能非常强大的监测及故障排除工具。使用 show 命令可以实现以下多种功能。

（1）监测路由器在最初安装时的工作情况。

（2）监测正常的网络运行状况。

（3）分离存在问题的接口、节点、介质或者应用程序。

（4）确定网络是否出现拥塞现象。

（5）确定服务器、客户机以及其他邻接设备的工作状态。

以下为 show 命令最常用的一些形式。

- show version：显示系统硬件、软件版本，配置文件的名称和来源以及引导图像的配置。
- show running-config：显示当前正在运行的路由器所采用的配置情况。
- show startup-config：显示保存在非易失随机存储器（NVRAM）中的路由器配置信息。
- show interfaces：显示配置在路由器或者访问服务器上的所有接口的统计信息。这一命令的输出信息根据网络接口所在的网络的配置类型不同而有所不同。
- show controllers：显示网络接口卡控制器的统计信息。
- show flash：显示闪存的布局结构和信息内容。
- show buffers：显示路由器上的缓冲池的统计信息。
- show memory summary：显示存储池统计信息，以及关于系统存储器分配符的活动信息，并给出从数据块到数据块的存储器使用程序清单。

- show process cpu：显示路由器上活动进程的有关信息。
- show stacks：显示进程或者中断例程的堆栈使用情况，以及最后一次系统重新启动的原因。
- show debugging：显示关于排除故障类型的信息（路由器允许此种故障类型）。还可以使用许多其他的 show 命令。

关于使用 show 命令的细节，可以参阅相关设备的命令参考手册。

2）debug

利用 debug 特权命令可以查看到大量有用的信息，其中包括网络接口上可以看到的（或无法看到的）通信过程、网络节点产生的错误信息、特定协议的诊断数据包以及其他有用的故障排除数据。

debug 命令可以用于故障的定位，但是不能用于监测网络的正常运行状况。这是因为 debug 命令需要占用处理器的大量时间，可能打断路由器的正常操作。因此，应该在寻找特定类型的数据包或通信故障，并且已经将引发故障的原因缩小到尽可能小的范围内时，才使用 debug 命令。

不同形式的 debug 命令所输出的格式也大不相同：有些命令对每一数据包都产生一行输出信息，而有些命令对每一数据包产生多行输出信息；有些命令产生大量的输出信息，而有些命令只是偶尔才有输出信息；一些命令产生文本行，而另一些命令产生格式信息。

如果需要将 debug 命令的输出信息保存起来，那么可以将其输出信息保存到文件之中。在许多情况下，使用第三方厂商提供的诊断工具更为有效，也比使用 debug 命令带来的负面影响要小。

3）ping

利用 ping 命令，可以检查目的主机可否到达以及网络的连通性。ping 命令可以在 AppleTalk、ISO 无连接网络服务（ISO ConnectionlessNetwork Service，CLNS）、IP、Novell、Apollo、VINES、DECnet 以及 XNS 等多种网络中测试基本的网络连通性。

对于 IP 网络来说，ping 命令发送 Internet 控制报文协议（Internet Control Message Protocol，ICMP）的 Echo 报文。ICMP 协议能够报告错误信息，并且能够提供有关 IP 数据包寻址的信息。如果某一站点收到 ICMP 协议的 Echo 报文，那么它会向源节点发送一个 ICMP Echo 应答（ICMP Echo Reply）消息。

利用 ping 命令的扩展模式可以指定 IP 报头的选项。这样就使得路由器可以进行更为完善的测试。在 ping 命令的扩展命令提示符下输入 yes，就可以进入 ping 命令的扩展模式。

在网络正常工作时，使用 ping 命令查看该命令是如何在正常情况下起作用的，这样当进行故障排除时就可以与正常情况进行比较。

4）trace

trace 命令能显示出发出的分组向目的地传送时所走的路线。当数据包超过其生命周期（Time to Live，TTL)数值时，将会产生出错信息，trace 命令就是利用这一机制实现的。首先，发送 TTL 数值为 1 的探测包。这将导致路径上的第一个路由器丢弃该探测包并返回“超时（time exceeded)”错误信息。随后，trace 命令继续发送几个探测包，并为其分别显示探测包的往返时间。每经过 3 次探测后，TTL 值加 1。每个送出的分组能产生两个错误消息中的一个。“超时”错误信息表明，路径中的路由器已经收到该探测包并将其丢弃。“端口不可达（port unreachable)”错误信息表明，目的节点已经收到该探测包，但是由于目的节点无法将其提交给相应的进程而将其丢弃。如果在接收到应答信息之前定时器出现超时，那么 trace 命令将显示为星号（*)。当接收到目的节点的应答信息时，或者当 TTL 数值超过了允许的最大值时，或者当用户中断 trace 进程时，trace 命令就结束了。

与 ping 命令一样，当网络正常工作时查看 trace 命令是如何在正常情况下起作用的，这样当进行故障排除时就可以与正常情况进行比较。

2．网络管理工具

一些厂商推出的网络管理工具如 Cisco Works、HP OpenView 等都含有监测以及故障排除功能，这有助于对网络互联环境的管理和故障的及时排除。下面以 Cisco Works 2000 为例介绍网络管理工具对排除网络故障的主要功能。

（1）Cisco View 提供动态监视和故障排除功能，包括 Cisco 设备、统计信息和综合配置信息的图形显示。

（2）网络性能监视器（Internetwork Performance Monitor，IPM）使网络工程师能够利用实时和历史报告主动地对网络响应进行故障诊断与排除。

（3）TrafficDirector RMON 应用程序是一个远程监测工具，它能够收集数据、监测网络活动并查找潜在的问题。

（4）VlanDirector 交换机管理应用程序是一个针对 VLAN（虚拟局域网）的管理工具，它能够提供对 VLAN 的精确描绘。

3．专用故障排除工具

在许多情况下，专用故障排除工具可能比设备或系统中集成的命令更有效。例如，在网络通信负载繁重的环境中，运行需要占用大量处理器时间的 debug 命令将会对整个网络造成巨大影响。然而，如果在“可疑”的网络上接入一台网络分析仪，就可以尽可能少地干扰网络的正常工作，并且很有可能在不打断网络正常工作的情况下获取到有用的信息。下面为一些典型的用于排除网络故障的专用工具。

（1）欧姆表、数字万用表及电缆测试器可以用于检测电缆设备的物理连通性。

（2）时域反射计（Time Domain Reflectors，TDR）与光时域反射计（Optical Time Domain Reflectors，OTDR）可以用于测定电缆断裂、阻抗不匹配以及电缆设备其他物理故障的具体位置。

（3）断接盒（breakout boxes）、智能测试盘和位/数据块错误测试器（BERT/BLERT）可以用于外围接口的故障排除。

（4）网络监测器通过持续跟踪穿越网络的数据包，能每隔一段时间提供网络活动的准确图像。

（5）网络分析仪（例如，NAI 公司的 Sniffer）可以对 OSI 所有7层上出现的问题进行解码，自动实时地发现问题，对网络活动进行清晰的描述，并根据问题的严重性对故障进行分类。

1）欧姆表、数字万用表及电缆测试器

欧姆表、数字万用表属于电缆检测工具中比较低档的一类。这类设备能够测量诸如交直流电压、电流、电阻、电容以及电缆连续性之类的参数。利用这些参数可以检测电缆的物理连通性。

电缆测试器（扫描器）也可以用于检测电缆的物理连通性。电缆测试器适用于屏蔽双绞线（STP）、非屏蔽双绞线（UTP）、10BaseT、同轴电缆及双芯同轴电缆等。通常，电缆测试器能够提供下述的功能。

（1）测试并报告电缆状况，其中包括近端串音（Near End Crosstalk，NEXT）、信号衰减及噪音。

（2）实现 TDR、通信检测及布线图功能。

（3）显示局域网通信中媒体访问控制（Media Access Control，MAC）层的信息，提供诸如网络利用率、数据包出错率之类的统计信息，完成有限的协议测试功能（例如，TCP/IP 网络中的 ping 测试）。

对于光缆而言，也有类似的测试设备。由于光缆的造价及其安装的成本相对较高，因此在光缆的安装前后都应该对其进行检测。对光纤连续性的测试需要使用可见光源或反射计。光源应该能够提供三种主要波长（即 850nm、1300nm 和 1550nm）的光线，配合能够测量同样波长的功率计一起使用，便可以测出光纤传输中的信号衰减与回程损耗。

2）时域反射计与光时域反射计

电缆检测工具中比较高档的就是时域反射计。这种设备能够快速地定位金属电缆中的断路、短路、压接、扭接、阻抗不匹配及其他问题。

TDR 的工作原理基于信号在电缆末端的振动。电缆的断路、短路及其他问题会导致信号以不同的幅度反射回来。TDR 通过测试信号反射回来所需要的时间，就可以计算出电缆中出现故障的位置。TDR 还可以用于测量电缆的长度。有些 TDR 还可以基于给定的电缆长度计算出信号的传播速度。

对于光纤的测试则需要使用光时域反射计。OTDR 可以精确地测量光纤的长度、定位光纤的断裂处、测量光纤的信号衰减、测量接头或连接器造成的损耗。OTDR 还可以用于记录特定安装方式的参数信息（例如，信号的衰减以及接头造成的损耗等）。以后当怀疑网络出现故障时，可以利用 OTDR 测量这些参数并与原先记录的信息进行比较。

3）断接盒、智能测试盘和位/数据块错误测试器

断接盒、智能测试盘和位/数据块错误测试器是用于测量PC、打印机、调制解调器、信道服务设备/数字服务设备（CSU/DSU）以及其他外围接口数字信号的数字接口测试工具。这类设备可以监测数据线路的状态，俘获并分析数据，诊断数据通信系统中常见的故障。通过监测从数据终端设备（DTE）到数据通信设备（DCE）的数据通信，可以发现潜在的问题、确定位组合模式、确保电缆铺设结构的正确。这类设备无法测试诸如以太网、令牌环网及FDDI之类的媒体信号。

4）网络监测器

网络监测器能够持续不断地跟踪数据包在网络上的传输，能够提供任何时刻网络活动的精确描述或者一段时间内网络活动的历史记录。网络监测器不会对数据帧中的内容进行解码。网络监测器可以对正常运作下的网络活动进行定期采样，以此作为网络性能的基准。

网络监测器可以收集诸如数据包长度、数据包数量、错误数据包的数量、连接的总体利用率、主机与MAC地址的数量、主机与其他设备之间的通信细节之类的信息。这些信息可以用于概括局域网的通信状况，帮助用户确定网络通信超载的具体位置、规划网络的扩展形式、及时地发现入侵者、建立网络性能基准、更加有效地分散通信量。

5）网络分析仪

网络分析仪（network analyzer）有时也称为协议分析仪（protocol analyzer），它能够对不同协议层的通信数据进行解码，以便于阅读的缩略语或概述形式表示出来，详细表示哪个层被调用（物理层、数据链路层等），以及每个字节或者字节内容起什么作用。

大多数的网络分析仪能够实现如下功能。

（1）按照特定的标准对通信数据进行过滤，例如，可以截获发送给特定设备及特定设备发出的所有信息。

（2）为截获的数据加上时间标签。

（3）以便于阅读的方式展示协议层数据信息。

（4）生成数据帧，并将其发送到网络中。

（5）与某些系统配合使用，系统为网络分析仪提供一套规则，并结合网络的配置信息及具体操作，实现对网络故障的诊断与排除，或者为网络故障提供潜在的排除方案。

2.8.3 网络故障分层诊断

1．物理层及其诊断

物理层是OSI分层结构体系中最基础的一层，它建立在通信媒体的基础上，实现系统和通信媒体的物理接口，为数据链路实体之间进行透明传输，为建立、保持和拆除计算机和网络之间的物理连接提供服务。

物理层的故障主要表现为设备的物理连接方式是否恰当；连接电缆是否正确。确定

路由器端口物理连接是否完好的最佳方法是使用 show interface 命令，检查每个端口的状态，解释屏幕输出信息，查看端口状态、协议建立状态和 EIA 状态。

2．数据链路层及其诊断

数据链路层的主要任务是使网络层无须了解物理层的特征而获得可靠的传输。数据链路层为通过链路层的数据进行打包和解包、差错检测和一定的校正能力，并协调共享介质。在数据链路层交换数据之前，协议关注的是形成帧和同步设备。查找和排除数据链路层的故障，需要查看路由器的配置，检查连接端口的共享同一数据链路层的封装情况。每对接口要和与其通信的其他设备有相同的封装。通过查看路由器的配置检查其封装，或者使用 show 命令查看相应接口的封装情况。

3．网络层及其诊断

网络层提供建立、保持和释放网络层连接的手段，包括路由选择、流量控制、传输确认、中断、差错及故障恢复等。排除网络层故障的基本方法是：沿着从源到目标的路径，查看路由器路由表，同时检查路由器接口的 IP 地址。如果路由没有在路由表中出现，应该通过检查来确定是否已经输入适当的静态路由、默认路由或者动态路由。然后手工配置一些丢失的路由，或者排除一些动态路由选择过程的故障，包括 RIP 或者 IGRP 路由协议出现的故障。例如，对于 IGRP 路由选择信息只在同一自治系统号（AS）的系统之间交换数据，查看路由器配置的自治系统号的匹配情况。

4．应用层及其诊断

应用层提供最终用户服务，如文件传输、电子信息、电子邮件和虚拟终端接入等。排除网络层故障的基本方法是：首先可在服务器上检查配置，测试服务器是否正常运行，如果服务器没有问题再检查应用客户端是否正确配置。

2.8.4　网络故障排除案例分析

1．案例一　光纤线路故障

一个新建的宿舍楼用户突然无法访问 Internet，出现问题的宿舍区与其他宿舍区都是通过光缆连接到机房的同一设备，其他的宿舍区都可以正常访问 Internet，说明机房的网络设备运转正常，而网管人员已经证明设置也没有问题，故初步判断故障是由物理层引起的。

1）初步查找故障原因

工程师携带测试仪器到达该市后，进一步对现场情况进行了解。这条光缆刚刚铺设不久，而且施工单位一个月前使用 OTDR（Optical Time Division Reflectometer，光纤测试器）对它进行了测试，并提供了完整的报告，所以运维部门并没有怀疑这次故障可能是由链路引起的。但根据长期从事测试工作所累积的经验，工程师坚持决定应该对这条光缆重新进行测试。

由于事先没有携带 OTDR，所以首先使用光损耗测试仪测试这条光缆的损耗是否在

允许范围之内，以此来判断链路是否存在故障。当工程师来到机房后发现，配线架上面所有的线缆都没有做标识，这给测试带来了很大的不便。为了避免因为盲目地断开连接器而导致业务中断，带来恶劣的影响，使用光纤识别器找出了连接到故障宿舍区的两根光纤。这种光纤识别器利用光纤的微弯损耗特性，可以在不损害连接的情况下找出正在使用的或特定的光纤，彻底解决了某些维护人员因错误地切断重要的光纤连接而产生严重后果的问题。

当工程师把光源和光功率计分别接在机房和宿舍的光纤接头上进行光功率测试时，发现光功率计的读数显示为 UNDER，这表示从光纤中传输过来的光信号功率太弱，以至于光功率计接收不到信号。可以确定这条链路肯定有问题。下面的工作就是通过进一步测试来确定故障的具体位置和原因。

2）锁定故障

会不会是由于连接器接头受到了污物的污染而造成接收端光功率过低呢？这也是光纤链路存在传输故障的主要原因之一。工程师使用光纤显微镜对所布的光纤以及两端的光纤跳线的端面进行了检测，未发现端面上有污物存在，可见故障并不是由于连接端面不洁净引起的。再使用可视故障定位仪分别从链路两端进行测试，这种设备可以发出能够传输 5km 远的高强度可视激光束，用来查找光纤链路是否存在断裂、过度弯曲和连接故障。我们从两地分别接入测试仪发出可视红光，在对端相互观察均没有发现有红光射出，而两地所用的光纤跳线上也没有红光泄漏的现象，说明光纤连接跳线是没有问题的。那么到此已经可以肯定故障点存在于光纤链路上。

最后使用了一种掌上型 OTDR 对光纤链路进行单端测试以对故障进行定位。这种最远测试距离为 20km 的仪器可以以数字的形式表示出光纤链路每个事件点的位置，由于不需要去看复杂的 OTDR 图形，所以使用起来非常简单方便，是局域网、城域网中传统 OTDR 的理想替代品。把设备接入光纤链路中，按动测试按钮，2s 后仪器显示数据说明距离测试端 520m 处光纤有一故障点。测试另一条光纤时显示同样信息，几乎可以肯定在那里的光纤已经因为某种原因遭到损坏，就是它造成宿舍区用户无法上网。

至此，引起网络故障的原因已经找到，下一步需进行光缆修复或更换光缆。同时针对网络管理上的欠缺需使用网络标识打印机和专用标签，按照 TIA/EIA-606 标准对其网络设备和布线系统进行重新规划管理，建立相应的备案文档。其后在更换了一条光缆后宿舍区用户已可以正常访问 Internet，至此这次所遇到的问题已经圆满解决。

3）故障结论

对于如今的光纤网络来说，再按照 TIA/EIA-568B 标准的规定只进行损耗的测试已经远远不能满足目前的需求了。只有在实际测试当中综合、合理地运用多种测试仪器，才能够得到链路全面的结果。对于已经测试过的光纤链路，也不能够保证它永远合格，所以建议对于光纤链路每半年进行一次性能检测。不要忽视网络标识管理在实际工作中的作用。

2．案例二　布线不符合标准

某政府部门内部办公网有一台服务器和 30 余台 PC，该网络拓扑结构为基于 Hub 的星型结构，共有 8 台 Hub（7 台 10M，1 台 10/100M），其中一台 10M Hub 为中心 Hub，其余分别级联于此 Hub 上。用户反映目前网络速度很慢，复制较大文件时经常会宕机，数据库访问速度慢。

1）测试准备

为完成对用户网络的测试，准备了美国 Fluke 683 企业级网络测试仪和 Fluke DSP-2000 电缆测试仪。

2）测试过程及分析

为了了解用户网络的流量特征，首先将 Fluke 683 企业级网络测试仪接入网络，进行网络运行的实时监测，进行系统的流量分析。当仪器一接入网络，就发现了网络流量存在异常状态，网络的带宽平均利用率（utilization）峰值达到了 60%，但其中碰撞（collision）平均占据了 25.9%，经过一段时间的连续测试，发现即使在没有过多流量的情况下，仅仅是广播都会带来 50%的碰撞，平均利用率仅为 5.04%，而平均冲突率却达到了 34.6%。可见，网络的有效利用率很低，碰撞消耗了很大的带宽资源。测试中并未发现帧级的错误。

为了能够对流量进行综合的了解，进行了半小时流量采样。带宽利用率分析图反映出用户网络流量随机性很大，在测试时间内最大利用率达到 61.7%，平均利用率为 10.2%。从碰撞分析图可以看出，碰撞的比例同网络利用率是成正比的，流量增加时，碰撞也随之增多，用户网络几乎每一时刻都伴随着大量的碰撞发生。流量综合分析图反映出整个测试过程中没有出现任何错误帧，广播流量非常少，并不存在广播风暴。可以看出，整个网络流量中有 1/3 的帧发生了碰撞。碰撞的比例大大超过以太网平均碰撞率小于 5%的建议，因而会降低网络的传输效率。

究竟是什么原因导致如此高的碰撞率呢？为了进一步确认问题根源，利用电缆测试仪对用户的部分电缆进行了认证测试。测试时选择了 TIA 五类通道（channel）链路模型标准（包含水平电缆及用户跳线），结果所有被检测链路均不合格，串扰（NEXT）远远超过标准。通过观察发现，几乎所有的电缆都未按照国际标准接线图进行打结，用户不正确的打结方式破坏了正常的双绞线对，导致了电缆内不同线对在传输信号时相互干扰（近端串扰）非常严重，这种干扰严重影响着数据的正常传输，轻则网络运行速度很慢，严重的会导致网络的瘫痪。

为了进一步确定电缆故障的范围，我们又分别对用户自己打结的电缆和建筑物内的综合布线进行了抽测，结果：用户电缆全部不合格，部分综合布线电缆不符合 TIA 标准，但其保证了传输和接收线对的双绞。至此，我们判断用户所反映的网络故障与其不规范的布线系统直接相关。

3）测试结论

通过上面对用户网络传输介质的测试以及网络运行时流量的综合分析，我们认为用户现有的网络性能缓慢是由大量的碰撞造成的，过多的碰撞占用了大量的有效传输时间，消耗了过多的带宽资源。而电缆的错误打结正是造成这一故障的根本原因。测试过程中未发现任何帧级错误以及服务器对请求的及时响应进一步排除了由于网络设备而引起的故障，因此建议用户对现有所有电缆重新按照标准打结（TIA 568B 接线图白/橙、橙、白/绿、蓝、白/蓝、绿、白/棕、棕）。对布线系统的整改后，网络速度明显提高，故障现象消失。

3．案例三　网络中形成环路

某单位局域网使用星型拓扑结构的千兆以太网技术，网络主干采用 1000Mbps 速率传输，中心机房配置一台华为 6506 三层路由交换机，各楼层使用华为 3026 或背板堆叠的 2026 接入核心交换机，各单位计算机通过直接接入或以级联方式通过接入层交换机接入网络。中心有多台服务器，提供文件服务、FTP 和 Web 等各项服务。全网分为 5 个 VLAN，根据不同的业务定义了不同网段的 IP 地址。随着信息访问需求的增加，接入网络的用户不断增多，在网络维护和建设中遇到过各种问题以及故障，现分析其中一个影响较大的故障，谈谈在网络管理和维护方面的一些经验和体会。

某日有多个用户反映网络连接情况时通时断，有时同一楼层的计算机都无法互相 ping 通，故障用户分布在多个楼层，故障点不集中。对个别端口做互换测试，故障仍然存在。在故障计算机上进行测试，发现可以 ping 通网络中的部分服务器或计算机，ping 核心交换机的 IP 地址常出现不通、丢包、时延大的现象。利用华为的网络软件对可管理的交换机做检查，没有明显的报错。

1）故障排查

首先怀疑为核心交换机物理故障。观察交换机的指示灯状态以及各端口的状态，显示正常。对核心交换机清除缓存、关闭重启，并检查交换机的配置情况，没有改变。

经过以上的检查和测试，分析故障应该不在硬件部分，利用 Sniffer 抓包分析软件将网络中的数据包抓下来分析，发现有大量数据包来自一个 MAC 地址，目的地址是根本不存在的 IP，怀疑是类似于“冲击波杀手”一类会造成网络堵塞的病毒。根据网络正常时建立的 IP 地址及 MAC 地址对应表查出该机属于某层的一个直属单位，初步确认故障点后将 MAC 地址对应的计算机从网络中断开并升级杀毒软件，然后重新接入网络，此时故障仍然存在。

为了确定具体故障点，要求该单位提供其接入拓扑图分析，发现该单位将分属于两个不同 VLAN 的连线分别连接两个不同的 Hub，当天为了使用方便，将两个 Hub 用级联的方式连接到了一起，将其连线断开后，故障彻底排除。

2）故障原因

此次故障原因主要是由于网络中有环路存在，造成每一帧都在网络中重复广播，引起了广播风暴。要消除这种网络循环连接带来的网络广播风暴可以使用 STP 协议（生成

树协议），以网络中一台交换机为节点生成一棵转发树，而树是没有环路的，这样所有的数据都只在这棵树所指示的路径上传输，就不会产生广播风暴，但由于 STP 算法的开销非常大，所以交换机上都未启用该协议。

为避免在接入层出现同样的故障，从而影响整个局域网络用户的使用，所以在接入层启用树生成协议是必要的，或者在诊断故障时可以打开 SPT 协议协助确定故障点。

3）故障结论

在故障发生时，应首先了解故障前网络的改动，建立完善的网络文档资料。包括网络布线图、IP 及 MAC 对应表等，否则在确定 MAC 地址端口时会消耗大量的时间。现在有很多局域网工具软件都可以通过扫描获取网络中计算机的这些信息，如 LanExplorer 等。

4．案例四　病毒引起路由器过载

故障发生地的拓扑结构：使用一台 EnterasysSSR8000 作为边界路由器，同时也用它把校园内部划分为 8 个虚网，每个虚网各有一个堆叠的二层交换机作为台式计算机和笔记本计算机的接入设备，主干为千兆位，百兆位到桌面。

某日接到一个用户的求助电话，说他的机器不能上网了。这个用户的主机所在的虚网和网络中心不在同一个虚网中。用户介绍说 5 分钟前还是好的（能够上网），现在不知道为什么就不能上网了。而且他的机器（安装的系统为 Windows XP）最近没有安装什么新的程序，没有移动过计算机，也没有拔过网线。

1）故障排查

首先，排查网络客户端的错误配置。进入 MSDOS 方式使用 IPCONFIG 命令检查主机的 IP 地址配置，从主机向网关发送的数据包，全部都得到了回应，线路是连通的。打开浏览器，也能够正常上网，一点儿都没问题。现在的网络是正常的。正在怀疑的时候，发现网络又不通了。发现 ping 出的数据包未能到达网关。把台式计算机上的网线插到笔记本计算机上，配置好 IP 地址后 ping 网关，也出现时断时续的情况。断开的现象大概持续了 50s，然后又恢复正常。这基本可以排除是主机存在问题了，因为两台不相干主机同时出现此类问题的几率几乎为 0。鉴于此现象，首先排除了连接线缆的故障，因为连接的线缆不可能出现这种时断时续的情况，故障最有可能出在线缆的另一端——二层交换机上。于是来到这栋楼的设备间，查看交换机的状态，这是一个由两台交换机进行的堆叠，其中一台交换机上有一个上连的千兆端口。把笔记本计算机接到交换机的其中一个端口上，再 ping 网关。还是同样的故障，而且还发现每过 4～10 分钟，网络就会断一次，并且 40～50s 后又恢复正常。经过观察发现：没有发现端口指示灯的异常情况，说明交换机的各个端口均正常。把交换机重启一下。重启后，故障依旧。最后判断有可能是连接虚网的路由器出了问题。

问题集中到路由器上了，从路由器的外部指示灯上看，没什么异常现象。在网管机上 ping 路由器的地址（网管机是直接连在路由器的百兆模块上的），也是时通时断。又

继续观察了一段时间，发现每过4～10分钟，路由器所有模块的指示灯都会同时熄灭，接着控制模块上的HBT灯闪烁，然后OK灯亮起，最后所有模块的指示灯均显示Online。HBT灯闪烁表示路由器正在启动，也就是说正在自动重启，而且40s左右的网络断开时间正好是路由器的重启所需的时间。现在问题的查找工作已经结束，肯定是路由器出了故障。

在路由器正常工作的时候，把笔记本计算机的COM口使用路由器的专用CONSOLE线连接起来，建立超级终端。在管理模式下使用命令show bootlog查看系统的启动记录，发现各个模块的加载均属正常。造成路由器重启的原因，最大的可能就是CPU的利用率达到100%。使用show cpu-utilization命令查看CPU的使用率。

CPU Utilization（5 seconds）：50%（60 seconds）：60%（前者是指5s内CPU平均使用率为50%，后者是60s内CPU平均使用率为60%）

连续使用此命令后，得知CPU利用率正在逐渐上升，当达到95%的时候路由器便自动重启。看来路由器的负载太大了，因为平时正常情况下，CPU的使用率仅为1%～6%。当网络使用高峰期的时候CPU的利用率会稍微高一点。但到底是什么让路由器过载呢？幸好以前曾经给路由器设置过日志记录，并把日志发送到一个日志服务器上。但是打开这台服务器所记录的日志并未能找到有用的线索。因为当路由器负载过大时，它已经不能往日志服务器上发送日志了，只能用system show syslog buffer命令来查看当前系统缓存中的日志记录：

```
2003-09-10 09:28:32 %ACL_LOG-I-DENY,
ACL [out] on "uplink" ICMP 210.16.3.82 -> 210.55.37.72
2003-09-10 09:28:32 %ACL_LOG-I-PERMIT,
ACL [out] on "uplink" ICMP 210.16.3.82 -> 61.136.65.13
2003-09-10 09:28:32 %ACL_LOG-I-DENY,
ACL [out] on "uplink" ICMP 210.16.3.82 -> 202.227.100.65
2003-09-10 09:28:32 %ACL_LOG-I-DENY,
ACL [out] on "uplink" ICMP 210.16.3.82 -> 193.210.224.202
2003-09-10 09:28:32 %ACL_LOG-I-DENY,
ACL [out] on "uplink" ICMP 210.16.3.82 -> 218.32.21.101
```

2）故障原因

很明显，210.16.3.82这台在使用ICMP协议向其他主机发起攻击。据此判断，这台主机很可能中毒。鉴于情况分析，可能是网络中存在中了“冲击波杀手”病毒的主机。该病毒使用类型为echo的ICMP报文来ping根据自身算法得出的IP地址段，以此检测这些地址段中存活的主机，并发送大量载荷为aa，填充长度为92字节的icmp报文，从而导致网络堵塞。而且病毒一旦发现存活的主机，便试图使用135端口的rpc漏洞和80端口的webdav漏洞进行溢出攻击。溢出成功后会监听69（TFTP专业端口，用于文件下

载）端口和 666～765（通常是 707 端口）范围中的一个随机端口等待目标主机回连。

3）故障处理

根据该病毒的传播机理，立刻在路由器上设置访问控制列表（ACL），以阻塞 UDP 协议的 69 端口（用于文件下载）、TCP 的端口 135（微软的 DCOM RPC 端口）和 ICMP 协议（用于发现活动主机）。最后再把这个 ACL 应用到上连接口（uplink）上。这样就可以把"冲击波杀手"从网络的出口处堵截住。为了防止已经感染"冲击波杀手"的主机在校内各个虚网之间传播，还要把这个 ACL 应用到校内各虚网的接口上。这时使用并查看 CPU 的使用率，恢复到了正常状态，等待一段时间后，没有出现重启现象。至此，路由器故障全部解决。

4）故障结论

由于路由器不能自动丢弃这种病毒发出的攻击数据包，而导致了路由器重启，应配置一定的安全措施来避免这类问题的发生。为了彻底解决问题，还应升级路由器的 IOS。与设备供应商取得联系并获得最新的 IOS 映像文件。

第 3 章　网络资源设备

本章介绍了网络上的服务器、存储系统和利用网络的传真、打印以及视频会议系统。

3.1　网络服务器

按服务器的处理器架构(即服务器 CPU 所采用的指令系统)可把服务器划分为 RISC 架构服务器和 IA 架构服务器。后者包括 CISC 架构服务器和 VLIW 架构服务器两种。

3.1.1　RISC 架构服务器

RISC（Reduced Instruction Set Computing，精简指令集）的指令系统相对简单，只要求硬件执行很有限且最常用的那部分指令，大部分复杂的操作则使用成熟的编译技术，由简单指令合成。目前在中高档服务器特别是高档服务器中普遍采用 RISC 指令系统的 CPU。RISC 架构服务器采用的是封闭的发展策略，即由单个厂商提供垂直的解决方案，从服务器的系统硬件到系统软件都由这个厂商完成。RISC 处理器发展至今，主要的 RISC 处理器芯片生产商有 Sun 公司、Fujitsu 公司的 SPARC 系列处理器，IBM 公司的 Power 系列处理器，HP 公司的 PA-RISC，HP 公司（Compaq 被收购之前）的 Alpha 处理器及 MIPS 公司的 MIPS 等。

RISC 架构的服务器除处理器各不相同外，I/O 总线也不相同。Fujitsu 是 PCI，Sun 是 SBUS 等，这就意味着不同厂商 RISC 机器上的插卡，如网卡、显示卡和 SCSI 卡等可能也是专用的。操作系统一般是基于 UNIX 的，像 Sun、Fujitsu 是用 Sun Solaris，HP 是用 HP-UNIX，IBM 是 AIX 等，所以 RISC 架构的服务器是相对封闭专用的计算机系统。使用该架构的用户一般是看中 UNIX 操作系统的安全性、可靠性和专用服务器的高速运算能力。

随着 Internet 的飞速发展，基于 RISC 处理器的 UNIX 服务器市场经历过快速的增长。但近几年，UNIX 市场在慢慢地萎缩，部分市场慢慢被 AMD Opteron 处理器、英特尔至强、安腾所取代。但到目前，RISC 处理器仍然占据相当可观的市场份额，IBM、Sun 和 HP 三大厂商在近几年 UNIX 领域的白热化竞争，说明这块仍然得到了服务器巨头的重视。

3.1.2　IA 架构服务器

IA 架构的服务器采用了开放体系结构，有大量的硬件和软件的支持者。在这个阵营

中，主要的技术领头者是最大的 CPU 制造商 INTEL，国外著名的 IA 服务器制造商有 IBM、HP 和 Dell 等，国内主要的 IA 架构服务器的制造商有联想、浪潮和曙光等。

1．CISC 架构

从计算机诞生以来，人们一直沿用 CISC（Complex Instruction Set Computing，复杂指令系统计算）指令集方式。早期的桌面软件是按 CISC 设计的，并一直延续到现在，所以，微处理器（CPU）厂商一直在走 CISC 的发展道路，包括 Intel、AMD，还有其他一些现在已经更名的厂商，如 TI（德州仪器）、Cyrix 以及 VIA（威盛）等。在 CISC 微处理器中，程序的各条指令是按顺序串行执行的，每条指令中的各个操作也是按顺序串行执行的。顺序执行的优点是控制简单，但计算机各部分的利用率不高，执行速度慢。

CISC 架构的服务器主要以 IA-32 架构（Intel Architecture，英特尔架构）为主，而且多数被中低档服务器所采用。如果企业的应用都是基于 NT 平台的应用，那么服务器的选择基本上就定位于 IA 架构（CISC 架构）的服务器。如果企业的应用主要是基于 Linux 操作系统，那么服务器的选择也是基于 IA 结构的服务器。

2．VLIW 架构

VLIW（Very Long Instruction Word，超长指令集架构）架构采用了先进的 EPIC（Explicitly Parallel Instruction Computing，清晰并行指令）设计，业界也把这种构架叫做“IA-64 架构”。每时钟周期例如 IA-64 可运行 20 条指令，而 CISC 通常只能运行 1～3 条指令，RISC 能运行 4 条指令，可见，VLIW 要比 CISC 和 RISC 强大得多。VLIW 的最大优点是简化了处理器的结构，删除了处理器内部许多复杂的控制电路，这些电路通常是超标量芯片（CISC 和 RISC）协调并行工作时必须使用的，VLIW 的结构简单，能够使其芯片制造成本降低，价格低廉，能耗少，而且性能也要比超标量芯片高得多。目前，基于这种指令架构的微处理器主要有 Intel 的 IA-64 和 AMD 的 x86-64 两种。

2002 年 7 月 8 日，英特尔公司推出其 EPIC 处理器微体系机构的第二代处理器，即英特尔安腾 2 处理器。英特尔安腾 2 处理器拥有许多新特性，可显著提升性能速度，与大量 RISC 厂商面向服务器提供的最先进的处理器展开市场争夺战。

目前，安腾解决方案联盟（ISA）的所有服务器制造商会员，其中包括布尔、富士通、惠普、富士通西门子计算机、英特尔、日立、NEC 和 SGI，都将相应推出基于双核英特尔安腾 9100 系列处理器的产品。RISC 结构的产品目前受到安腾的冲击是毋庸置疑的。一个典型例子是：HP 9000 的核心处理器采用的是 HP 自主研发的 RISC 结构的 PA-8900 处理器，主要针对 HP-UX 操作系统。不可否认，PA-8900 处理器是一款设计非常成功的 RISC 处理器，但由于 UNIX 市场不断缩小，惠普已开始决定放弃对该处理器继续开发，以后将使用安腾处理器来代替 PA-8900 处理器。

3.1.3　性能要求及配置要点

1．性能要求

网络服务器是整个网络的核心，如何选择与本网规模相适应的服务器，是有关决策

者和技术人员都要考虑的问题。下面是选择网络服务器应当注意的事项。

（1）性能要稳定。为了保证网络能正常运转，选择的服务器首先要确保稳定，因为一个性能不稳定的服务器，即使配置再高、技术再先进，也不能保证网络正常运转，严重的可能给使用者造成难以估计的损失。另外一方面，性能稳定的服务器还意味着为单位节省维护费用。

（2）以够用为准则。由于本身的信息资源以及资金实力有限，不可能一次性投资太多的经费去采购档次很高、技术很先进的服务器。对于建设单位而言，最重要的是根据实际情况，并参考以后的发展规划，有针对性地选择满足目前信息化建设的需要又不投入太多资源的解决方法。

（3）应考虑扩展性。由于网络处于不断发展之中，快速增长的应用不断对服务器的性能提出新的要求，为了减少更新服务器带来的额外开销和对工作的影响，服务器应当具有较高的可扩展性，可以及时调整配置来适应发展。

（4）要便于操作管理。如果服务器产品具有良好的易操作性和可管理性，当出现故障时无须厂商支持也能排除。便于操作和管理，主要是指用相应的技术来提高系统的可靠性能，简化管理因素，降低维护费用成本。

（5）满足特殊要求。不同网络应用侧重点不同，对服务器性能的要求也不一样。例如，VOD 服务器要求具有较高的存储容量和数据吞吐率，而 Web 服务器和 E-mail 服务器则要求 24 小时不间断运行。如果网络服务器中存放的信息有敏感资料，就要求选择的服务器有较高的安全性。

（6）配件搭配合理。为了能使服务器更高效地运转，要确保购买的服务器的内部配件的性能必须合理搭配。例如，购买了高性能的服务器，但是服务器内部的某些配件使用了低价的兼容组件，就会出现有的配件处于瓶颈状态，有的配件处于闲置状态，最后的结果是整个服务器系统的性能下降。一台高性能的服务器不是一件或几件设备的性能优异，而是所有部件的合理搭配。要尽量避免小马拉大车，或者是大马拉小车的情况。低速、小容量的硬盘，小容量的内存，任何一个产生系统瓶颈的配件都有可能制约系统的整体性。

（7）理性看待价格。无论购买什么产品，用户都会很看重产品的价格。当然，一分价钱一分货，高档服务器的价格比低档服务器的价格高是无可非议的事情。但对于一些应用来说，不一定非得购买那些价格昂贵的服务器，尽管高端服务器功能很多，但是这些功能对普通应用来说使用率不高。性能稳定、价格适中的服务器应该是建设单位建设网络的理性选择。

（8）售后服务要好。由于服务器的使用和维护包含一定的技术含量，这就要求操作和管理服务器的人员必须掌握一定的使用知识。因此，选择售后服务好的 IT 产品，应该成为建设单位明智的决定。

2. 配置要点

目前最基本的服务器应用有数据库服务器、文件服务器、Web 服务器、邮件服务器、多媒体服务器和终端服务器等。这些应用对于服务器配置要求的侧重点不同，根据不同应用采购不同配置的服务器可以使服务器资源得到充分利用，避免资金和服务器资源的浪费。在下文中将逐一对这几种服务器的配置需求侧重点进行分析，为企业提供参考。

1）数据库服务器

在企业的信息化建设中，数据库是最为广泛的一种应用。构建数据库服务器可以将企业内部数据合理进行存储和组织，使企业信息的检索和查询执行更为高效。目前主流应用的数据库产品有 IBM DB2、Oracle、微软 SQL server、MySQL 和 Sybase 等。

数据库服务器对系统各个方面要求都很高，要处理大量的随机 I/O 请求和数据传送，对内存、磁盘以及 CPU 的运算能力均有一定的要求。内存方面，数据库服务器需要高速高容的内存来节省处理器访问硬盘的时间，提高服务器的响应速度。同时，一些数据库产品如 Oracle 对于硬件的要求比较高，如安装 Windows 版本的 Oracle 10G 要求至少需要 1GB 的物理内存。

在磁盘方面，高速的磁盘子系统也可以提高数据库服务器查询应答的速度，这就要求磁盘具有高速的接口和转速，目前主流应用的存储介质有 10k 或者 15k 转的 SCSI 硬盘或 SAS 硬盘等。

数据库服务器对于处理器性能要求也很高。数据库服务器需要根据需求进行查询，然后将结果反馈给用户。如果查询请求非常多，例如大量用户同时查询的时候，如果服务器的处理能力不够强，无法处理大量的查询请求并做出应答，那么服务器可能会出现应答缓慢甚至死机的情况。

综上，数据库服务器对于硬件需求的优先级为内存、磁盘、处理器（三者在满足合理搭配的前提下）。

2）文件服务器

文件服务器是用来提供网络用户访问文件、目录的并发控制和安全保密措施的局域网服务器。首先，文件服务器要承载大容量数据在服务器和用户磁盘之间的传输，因此对于网速具有较高要求。

其次是对磁盘的要求比较高，文件服务器要进行大量数据的存储和传输，所以对磁盘子系统的容量和速度都有一定的要求。选择高转速、高接口速度、大容量缓存的磁盘，并且组建磁盘阵列，可以有效提升磁盘系统传输文件的速度。

除此之外，大容量的内存可以减少读写硬盘的次数，为文件传输提供缓冲，提升数据传输速度。文件服务器对于 CPU 等其他部件的要求不是很高。

综上，文件服务器对于硬件需求的优先级为网络系统、磁盘系统和内存。

3）Web 服务器

不同的网站内容对于 Web 服务器硬件需求也是不同的，如果 Web 站点是静态的，

对 Web 服务器硬件要求从高到低依次是网络系统、内存、磁盘系统、CPU。如果 Web 服务器上要进行密集计算（例如，动态产生 Web 页），则对服务器硬件需求依次为内存、CPU、磁盘子系统和网络系统。

4）邮件服务器

邮件服务器是对实时性要求不高的一个系统，对于处理器性能要求不是很高，但是由于要支持一定数量的并发连接，对于网络子系统和内存有一定的要求。邮件服务器软件对于内存需求也较高。同时，邮件服务器需要较大的存储空间来存储邮件及一些文件，但是对中小企业来说，企业邮箱的数量一般只在几百个以下，所以对于服务器的配置要求并不高，一台入门级的服务器完全可以承载几百个邮件客户端的需求。

邮件服务器对于硬件要求的优先程度依次为内存、磁盘、网络系统、处理器。

5）终端服务器

终端服务器是实现集中化应用程序访问的一种服务器。使用终端服务的客户可以在远程以图形界面的方式访问服务器，并且可以调用服务器中的应用程序、组件和服务等，和操作本机系统一样。这样的访问方式不仅大大方便了各种各样的用户，而且大大地提高了工作效率，并且能有效地节约企业的成本。

终端服务器由于是将客户端的所有负载均加在服务器端，所以对于服务器的处理能力有一定的要求，处理器要可以承载一定数量的并发请求，提供快速的响应速度，如果处理能力不够，容易造成服务器响应缓慢、软件运行错误甚至宕机的情况。高速大容量的内存可以提高终端服务器的响应速度，也是提升整体性能的必要条件之一。由于终端服务器与客户端的数据传输量并不是很大，所以对于网络要求不是很高，并且终端服务器主要是应用于企业内部网络，内部高速的局域网环境完全可以满足终端服务器和客户端之间的带宽需求。

综上，终端服务器对于硬件要求的优先程度依次为处理器、内存、磁盘和网络系统。

总结：上文列出了几种最为常用的服务器角色对于硬件需求的优先级，从总体来看，因为这几种应用角色对服务器的处理器、内存、磁盘、网络系统的需求程度并不相同，所以在服务器规划选型的时候，不要一味地追求服务器的处理速度。举个例子来说，双路四核服务器的处理性能很强，但是用来做百余个客户端的邮件服务器或者静态 Web 服务器性能并不会比单路双核服务器优异多少，大部分的服务器资源都会被浪费掉。所以，在选购之初明确自身需求以及应用种类，对症下药才是明智之举。

服务器性能的量化指标一直是业内关注的问题。常见的量化指标有交易处理性能委员会（http://www.tpc.org）的联机事务处理性能指标 TPCC 值和标准性能评估公司（http://www.spec.org）的 Web、Java 等性能指标 SPEC 值，但是只有部分厂家的部分型号的服务器能够在这两个网站上查到性能指标。即使能查到，TPCC 值和 SPEC 值也只能作为服务器规划选型的参考。还有一个在 HPC 领域常用的性能指标 FLOPS（Floating-point Operations Per Second，每秒执行的浮点运算次数），反映的是一台服务器中 CPU 的

理论峰值性能，虽然 FLOPS 大大高于实际性能（即便是 LINPACK 值，通常也只是 FLOPS 的 40%～80%），但也可供参考使用。FLOPS 的计算公式是：

FLOPS=CPU 主频×CPU 核数×FPU 数（/核）×2

其中，“FPU 数（/核）”是一个 CPU 核中的浮点处理单元（FPU）数。

3.1.4　服务器相关技术

1．64 位计算

由于 x86 架构服务器 32 位计算能力的限制，使得“企业计算平台统一化”的进程在经历了前几年高速发展之后，开始遇到了瓶颈。64 位计算与 32 位计算的最大区别在于“寻址能力”和“数据处理能力”，64 位计算平台基于 64 位长的“寄存器”，提供比 32 位更大的数据带宽和寻址能力。

基于 x86 服务器的 Intel 至强处理器、AMD Opteron 以 64 位计算，有效解决了 32 位计算系统的瓶颈。同时，伴随新至强发布的 DDR2、PCI-EXPRESS 等芯片组的升级，也为系统性能整体的提升提供了有力支持。随着 Intel 和 AMD 同在低端服务器领域发起 64 位普及攻坚战，基于 x86 服务器的 64 位应用需求可能受到激发，相关应用增长就可能存在一个激增点。

2．双核和多核处理器

多核技术也称为芯片上多处理器技术（CMP），目前已经成为当前微处理器发展的方向。多内核的想法脱胎于摩尔定律（芯片上晶体管的数目每两年增加一倍）。过去，为了增加高速缓存（用于快速数据访问的集成的存储池）的尺寸，或者为了增强其他提高性能的部件（例如指令水平并行度，允许芯片每个时钟周期执行多个任务），经常要使用更多的晶体管。但是，现在芯片厂商用更多的晶体管来制造更多核心，以提高性能，这种方法不会显著增加芯片功耗。

3．PCI-E 技术

与传统 PCI 以及更早期的计算机总线的共享并行架构相比，PCI Express 采用设备间的点对点串行连接（serial interface）。即允许每个设备都有自己的专用连接，是独占的，并不需要向整个总线请求带宽；同时，利用串行的连接特点能将数据传输速度提高到 2.5Gbps 的单向单线连接的频率，达到远超出 PCI 总线的传输速率。针对不同的设备，可以实现 x1、x2、x4、x8、x12、x16 或 x32 灵活的配置，满足带宽的不同要求。串行连接还可以大大减少电缆间的信号和电磁干扰，由于传输线条数有所减少，更能节省空间和连接更远的距离，简化了 PCI 的设计，降低了系统成本。

4．ECC 内存技术

ECC（Error Checking and Correcting，错误检查和纠正）不是一种内存类型，只是一种内存技术。ECC 纠错技术也需要额外的空间来储存校正码，但其占用的位数跟数据的长度并非呈线性关系。

通俗地讲，一个 8 位的数据产生的 ECC 码要占用 5 位的空间，而一个 16 位的数据 ECC 码只需在原来基础上再增加一位，也就是 6 位；而 32 位的数据则只需再在原来的基础上增加一位，即 7 位的 ECC 码即可，依此类推。ECC 码将信息进行 8 位的编码，采用这种方式可以恢复 1 位的错误。每一次数据写入内存时，ECC 码使用一种特殊的算法对数据进行计算，其结果称为校验位（check bits）。然后将所有校验位加在一起的和是“校验和（check sum）”，校验和与数据一起存放。当这些数据从内存中读出时，采用同一算法再次计算校验和，并和前面的计算结果相比较，如果结果相同，说明数据是正确的；反之，说明有错误，ECC 可以从逻辑上分离错误并通知系统。当只出现单位错误时，ECC 可以把错误改正过来不影响系统运行。

除了能够检查到并改正单位错误之外，ECC 码还能检查到（但不改正）单 DRAM 芯片上发生的任意两个随机错误，并最多可以检查到 4 位的错误。当有多位错误发生时，ECC 内存会生成一个不可隐藏（non-maskable interrupt）的中断，会中止系统运行，以避免出现数据恶化。ECC 内存技术虽然可以同时检测和纠正单位错误，但如果同时检测出两个以上位的数据有错误，则无能为力。

5. 刀片服务器

刀片服务器是一种 HAHD（High Availability High Density，高可用高密度）的低成本服务器平台，是专门为特殊应用行业和高密度计算机环境设计的。其中，每一块“刀片”实际上就是一块系统主板，它可以通过本地硬盘启动自己的操作系统，如 Windows NT/2000、Linux 和 Solaris 等，类似于一个独立的服务器。在这种模式下，每一个主板运行自己的系统，服务于指定的不同用户群，相互之间没有关联。不过可以用系统软件将这些主板集合成一个服务器集群。在集群模式下，所有的主板可以连接起来提供高速的网络环境，可以共享资源，为相同的用户群服务。在集群中插入新的“刀片”，就可以提高整体性能。而由于每块“刀片”都是热插拔的，所以系统可以轻松地进行替换，从而便于进行升级、维护。

服务器集群作为一种实现负载均衡的技术，可以有效地提高服务的稳定性和核心网络服务的性能，还可以提供冗余和容错功能。理论上，服务器集群可以扩展到无限数量的服务器。无疑，服务器集群和 RAID 镜像技术的诞生为计算机和数据池的 Internet 应用提供了一个新的解决方案，其成本远远低于传统的高端专用服务器。但是，服务器集群的集成能力低，管理这样的集群使很多 IDC 都非常头疼。尤其是集群扩展的需求越来越大，维护这些服务器的工作量很大，包括服务器之间的内部连接和摆放空间的要求。这些物理因素都限制了集群的扩展。刀片服务器（Blade Server）的出现适时地解决了这样的问题。高密度服务器内置了监视器和管理工具软件，可以几十个甚至上百个地堆放在一起。配置一台高密度服务器就可以解决一台到一百台服务器的管理问题。如果需要增加或者删除集群中的服务器，只要插入或拔出一个 CPU 板即可。从这个意义上来说，Blade Server 克服了服务器集群的缺点。

6．SMP 技术

SMP（Symmetrical MultiProcessing，对称多处理）技术是相对非对称多处理技术而言的、应用十分广泛的并行技术。在这种架构中，多个处理器运行操作系统的单一复本，并共享内存和一台计算机的其他资源。所有的处理器都可以平等地访问内存、I/O 和外部中断。

在非对称多处理系统中，任务和资源由不同处理器进行管理，有的 CPU 只处理 I/O，有的 CPU 只处理操作系统的提交任务，显然非对称多处理系统是不能实现负载均衡的。在对称多处理系统中，系统资源被系统中所有 CPU 共享，工作负载能够均匀地分配到所有可用处理器之上。

目前，大多数 SMP 系统的 CPU 是通过共享系统总线来存取数据，实现对称多处理的。例如，某些 RISC 服务器厂商使用 Crossbar 或 Switch 方式连接多个 CPU，虽然性能和可扩展性优于 Intel 架构，但 SMP 的扩展性仍有限。

在 SMP 系统中增加更多处理器的难点是系统不得不消耗资源来支持处理器抢占内存，以及内存同步两个主要问题。抢占内存是指当多个处理器共同访问内存中的数据时，它们并不能同时去读写数据，虽然一个 CPU 正读一段数据时，其他 CPU 可以读这段数据，但当一个 CPU 正在修改某段数据时，该 CPU 将会锁定这段数据，其他 CPU 要操作这段数据就必须等待。

显然，CPU 越多，这样的等待问题就越严重，系统性能不仅无法提升，甚至下降。为了尽可能地增加更多的 CPU，现在的 SMP 系统基本上都采用增大服务器 Cache 容量的方法来减少抢占内存问题，因为 Cache 是 CPU 的“本地内存”，它与 CPU 之间的数据交换速度远远高于内存总线速度。又由于 Cache 支持不共享，这样就不会出现多个 CPU 抢占同一段内存资源的问题了，许多数据操作就可以在 CPU 内置的 Cache 或 CPU 外置的 Cache 中顺利完成。

然而，Cache 的作用虽然解决了 SMP 系统中的抢占内存问题，但又引起了另一个较难解决的所谓“内存同步”问题。在 SMP 系统中，各 CPU 通过 Cache 访问内存数据时，要求系统必须经常保持内存中的数据与 Cache 中的数据一致，若 Cache 的内容更新了，内存中的内容也应该相应更新，否则就会影响系统数据的一致性。由于每次更新都需要占用 CPU，还要锁定内存中被更新的字段，而且更新频率过高又必然影响系统性能，更新间隔过长也有可能导致因交叉读写而引起数据错误，因此，SMP 的更新算法十分重要。目前的 SMP 系统多采用侦听算法来保证 CPU Cache 中的数据与内存保持一致。Cache 越大，抢占内存再现的概率就越小，同时由于 Cache 的数据传输速度高，Cache 的增大还提高了 CPU 的运算效率，但系统保持内存同步的难度也很大。

在硬件方面，SMP 可以在 UltraSPARC、SPARC64、Alpha 以及 PowerPC 架构上实现，也可以利用包括 486 以上所有 Intel 芯片来实现。

7. 集群技术

集群（Cluster）技术是近几年兴起的发展高性能计算机的一项技术。它是一组相互独立的计算机，利用高速通信网络组成一个单一的计算机系统，并以单一系统的模式加以管理。其出发点是提供高可靠性、可扩充性和抗灾难性。一个集群包含多台拥有共享数据存储空间的服务器，各服务器通过内部局域网相互通信。当一台服务器发生故障时，它所运行的应用程序将由其他服务器自动接管。在大多数模式下，集群中所有的计算机拥有一个共同的名称，集群内的任一系统上运行的服务都可被所有的网络客户使用。采用集群系统通常是为了提高系统的稳定性和网络中心的数据处理能力及服务能力。

常见集群技术如下。

1）服务器镜像技术

服务器镜像技术是将建立在同一个局域网之上的两台服务器通过软件或其他特殊的网络设备（例如镜像卡）将两台服务器的硬盘做镜像。其中，一台服务器被指定为主服务器，另一台为从服务器。客户只能对主服务器上的镜像的卷进行读写，即只有主服务器通过网络向用户提供服务，从服务器上相应的卷被锁定以防对数据的存取。主/从服务器分别通过心跳监测线路互相监测对方的运行状态，当主服务器因故障宕机时，从服务器将在很短的时间内接管主服务器的应用。

服务器镜像技术的特点是成本较低，提高了系统的可用性，保证了在一台服务器宕机的情况下系统仍然可用。但是，这种技术仅限于两台服务器的集群，系统不具有可扩展性。

2）应用程序错误接管集群技术

错误接管集群技术是将建立在同一个网络里的两台或多台服务器通过集群技术连接起来，集群节点中的每台服务器各自运行不同的应用，具有自己的广播地址，对前端用户提供服务，同时每台服务器又监测其他服务器的运行状态，为指定服务器提供热备份服务。

错误接管集群技术通常需要共享外部存储设备，例如磁盘阵列柜，两台或多台服务器通过 SCSI 电缆或光纤与磁盘阵列柜相连，数据都存放在磁盘阵列柜上。这种集群系统中通常是两个节点互为备份的，而不是几台服务器同时为一台服务器备份，集群系统中的节点通过串口、共享磁盘分区或内部网络来互相监测对方的心跳。

错误接管集群技术经常用在数据库服务器、MAIL 服务器等的集群中。这种集群技术由于采用共享存储设备，所以增加了外设费用。它最多可以实现 32 台机器的集群，极大地提高了系统的可用性及可扩展性。目前在提高系统的可用性方面用得比较广泛的是应用程序错误接管技术，即通常所采用的双机通过 SCSI 电缆或光纤共享磁盘阵列的集群技术。

3）容错集群技术

容错集群技术的一个典型应用即容错机，在容错机中，每一个部件都具有冗余设计。

在容错集群技术中，集群系统的每个节点都与其他节点紧密地联系在一起，它们经常需要共享内存、硬盘、CPU 和 I/O 等重要的子系统。容错集群系统中各个节点被共同映像成为一个独立的系统，并且所有节点都是这个映像系统的一部分。在容错集群系统中，各种应用在不同节点之间的切换可以很平滑地完成，不需切换时间。

容错集群技术的实现往往需要特殊的软硬件设计，因此成本很高，但是容错系统最大限度地提高了系统的可用性，是财政、金融和安全部门的最佳选择。

8．模块化结构

模块化服务器主要包括计算模块、I/O 模块和海量存储器模块。这些模块协同工作，构成一个模块化服务器系统。在一个模块化服务器系统中，可以分别对每一个模块进行升级、故障查找，或用新模块替换旧模块，同类模块也可以随时加入到模块化服务器中，以便对系统进行扩展。

模块化服务器的最大好处之一，就是可以保护客户的投资。模块化服务器是一种可伸缩的服务器，客户可以随着业务需要，通过向服务器中添加各种模块，扩展他们的服务器系统；另一个显著优点是维护管理十分方便。模块化服务器增强了系统的可用性和容错性。从高性能多处理器计算机体系结构观点来看，ccNUMA 体系结构把多个处理器通过路由器光纤互联在一起，系统带宽可随系统规模扩大而增加，从而克服了基于总线的 SMP 体系结构所造成的瓶颈。ccNUMA 结构采用超立方体的多维互联特性，加上模块化计算所带来的灵活性，使系统的可伸缩性达到了前所未有的水平，同时节省了费用。因此，模块化的 NUMA 服务器在灵活性和经济性方面达到了一个新境界。

9．硬件分区

硬件分区，是将一台服务器的硬件分割成多个分区的体系结构。将服务器配置的处理器、内存和 I/O 控制器等硬件资源分配给多个分区，让各分区上运行不同的 OS，也就是提供“分区功能”。利用系统的硬件分区能力，系统可同时为多种不同操作系统提供支持，从而满足客户对相同物理硬件不断增长的需求。系统分区最初是静态的，当资源从一个分区移到另一个分区时，这两个分区中的应用和操作系统需要停止，在操作控制台对系统重新配置后，应用和操作系统才可以重新启动。随着操作系统进一步完善，操作系统在支持热插拔和热添加能力的同时，也为动态分区提供了所需要的支持基础。这就是说，资源可以在各个分区之间移动，而不会影响这一分区中的应用运行。

10．ISC

ISC（Intel Server Control，Intel 服务器控制）是一种网络监控技术，只适用于使用 Intel 架构的带有集成管理功能主板的服务器。采用这种技术后，用户在一台普通的客户机上就可以监测网络上所有使用 Intel 主板的服务器，监控和判断服务器是否“健康”。一旦服务器中机箱、电源、风扇、内存、处理器、系统信息、温度、电压或第三方硬件中的任何一项出现错误，就会报警提示管理人员。值得一提的是，监测端和服务器端之间的网络可以是局域网也可以是广域网，可直接通过网络对服务器进行启动、关闭或重

新置位，极大地方便了管理和维护工作。

11．EMP

EMP（Emergency Management Port，应急管理端口）是服务器主板上所带的一个用于远程管理服务器的接口。远程控制机可以通过 Modem 与服务器相连，控制软件安装于控制机上。远程控制机通过 EMP Console 控制界面可以对服务器进行下列工作。

（1）打开或关闭服务器的电源。

（2）重新设置服务器，甚至包括主板 BIOS 和 CMOS 的参数。

（3）监测服务器内部情况，如温度、电压和风扇情况等。

12．I2O

I2O（Intelligent Input/Output，智能输入输出）技术由于 PC 服务器的 I/O 体系源于单用户的 PC，而不是为处理大吞吐量任务的专用服务器而设计的，一旦成为网络中心设备后，数据传输量大大增加，因而 I/O 数据传输经常会成为整个系统的瓶颈。I2O 智能输入输出技术把任务分配给智能 I/O 系统，在这些子系统中，专用的 I/O 处理器将负责中断处理、缓冲存取以及数据传输等烦琐任务，这样系统的吞吐能力就得到了提高，服务器的主处理器也能被解放出来去处理更为重要的任务。因此，依据 I2O 技术规范实现的 PC 服务器在硬件规模不变的情况下能处理更多的任务，作为中小型网络核心的低端 PC 服务器可以从中获得更多的性能提高。

13．热插拔

热插拔（hot swap）功能就是允许用户在不关闭系统，不切断电源的情况下取出和更换损坏的硬盘、电源或板卡等部件，从而提高了系统对灾难的及时恢复能力、扩展性和灵活性等。例如，一些面向高端应用的磁盘镜像系统都可以提供磁盘的热插拔功能。如果没有热插拔功能，即使磁盘损坏不会造成数据的丢失，用户仍然需要暂时关闭系统，以便能够对硬盘进行更换。而使用热插拔技术，只要简单地打开连接开关或者转动手柄就可以直接取出硬盘，而系统仍然可以不间断地正常运行。

3.2 网络存储系统

3.2.1 SCSI 接口卡与控制卡

1．接口分类

硬盘接口是硬盘与主机系统间的连接部件，作用是在硬盘缓存和主机内存之间传输数据。每种接口协议拥有不同的技术规范，具备不同的传输速度，其存取效能的差异较大，所面对的实际应用和目标市场也各不相同。同时，各接口协议所处的技术生命阶段也各不相同，有些已经面临淘汰，有些则前景光明，但发展尚未成熟。因此，了解一款磁盘阵列的硬盘接口往往是衡量这款产品的关键指标之一。存储系统中目前普遍应用的

硬盘接口主要包括 SATA、SCSI、SAS 和 FC 等。

ATA（AT bus Attachment）硬盘在 SATA 硬盘出现前多用于家用产品。ATA 是广为使用的 IDE 和 EIDE 设备的相关标准，它是并行式的内部硬盘总线。

SATA（Serial ATA）是作为前期并行 ATA（PATA）的硬盘接口的升级技术而出现的，由于采用串行方式传输数据而知名。由于其具有成本低、数据传输速度高、可靠性强、扩配实现简单、减少系统布线的复杂度等优点，受到业界的重视和欢迎。随着 SATA 技术逐渐成熟，该标准的硬盘已经正式取代了传统的 PATA 硬盘，成为了中低端服务器的标准配置。与此同时，业界为了满足 SATA 硬盘的发展需要，在关键的芯片设计时，不仅考虑到 SATA 接口的连接，同时为了提高数据的传输性能和保证数据的安全性，提出了 SATA raid 技术。该技术不需要额外的硬件成本，就可以实现用户的数据保护和性能提升。

SCSI 接口的硬盘则主要应用于服务器市场。SAS（Serial Attached SCSI，串行连接 SCSI）是并行 SCSI 接口之后开发出的新一代 SCSI 技术。和现在流行的 SATA 硬盘相同，都是采用串行技术以获得更高的传输速度，并通过缩短连接线改善内部空间等。此接口的设计是为了改善存储系统的效能、可用性和扩充性，并且提供与 SATA 硬盘的兼容性。

FC（Fibre Channel，光纤通道）和 SCSI 接口一样，最初也不是为硬盘设计开发的接口技术，是专门为网络系统设计的，随着存储系统对速度的需求，才逐渐应用到硬盘系统中。FC 是为提高多硬盘存储系统的速度和灵活性才开发的，它的出现大大提高了多硬盘系统的通信速度。光纤通道的主要特性有热插拔性、高速带宽、远程连接和连接设备数量大等。

2．SCSI

SCSI（Small Computer System Interface，小型计算机系统接口）是一种专门为小型计算机系统设计的存储单元接口模式，通常用于服务器承担关键业务的较大的存储负载，价格也较贵。SCSI 计算机可以发送命令到一个 SCSI 设备，磁盘可以移动驱动臂定位磁头，在磁盘介质和缓存中传递数据，整个过程在后台执行。这样可以同时发送多个命令同时操作，适合大负载的 I/O 应用。在磁盘阵列上的整体性能大大高于基于 ATA 硬盘的阵列。

SCSI 规范发展到今天，已经是第六代技术了，从刚创建时的 SCSI（8 位）到今天的 Ultra 320 SCSI，速度从 1.2MBps 到现在的 320MBps，有了质的飞跃。目前的主流 SCSI 硬盘都采用了 Ultra 320 SCSI 接口，能提供 320MBps 的接口传输速度。SCSI 硬盘也有专门支持热拔插技术的 SCA2 接口（80-pin），与 SCSI 背板配合使用，就可以轻松实现硬盘的热拔插。目前在工作组和部门级服务器中，热插拔功能几乎是必备的。SCSI 性能参数如表 3-1 所示。

与 ATA 硬盘相比，SCSI 体现出了更适合中、高端存储应用的技术优势。

（1）SCSI 相对于 ATA 硬盘的接口支持数量更多。ATA 硬盘采用 IDE 插槽与系统连

接，而每个 IDE 插槽即占用一个 IRQ（中断号），而每两个 IDE 设备就要占用一个 IDE 通道，虽然附加 IDE 控制卡等方式可以增加所支持的 IDE 设备数量，但总共可连接的 IDE 设备数最多不能超过 15 个。而 SCSI 的所有设备只占用一个中断号，因此它支持的磁盘扩容量要比 ATA 多。

表 3-1　SCSI 性能参数比较

代		传输频率（MHz）	数据频宽（位）	传输率（MBps）	可连接设备（不含接口卡）
SCSI-1		5	8	5	7
SCSI-2	Fast	10	8	10	7
	Wide	10	16	20	15
SCSI-3	Ultra(Fast-20)	20	8	20	7
	Ultra Wide	20	16	40	15
	Ultra(Fast-40)	40	8	40	7
	Ultra2	40	16	40	15
	Ultra2	80	16	80	15
	Ultra160	80	16	160	15
	Ultra320	80	16	320	15

（2）SCSI 的带宽更宽。Ultra 320 SCSI 能支持的最大总线速度为 320MBps，虽然这只是理论值，但在实际数据传输率方面，即使最快的 ATA/SATA 硬盘和 SCSI 硬盘相比，无论在稳定性和传输速率上，都有一定的差距。不过如果单纯从速度的角度来看，用户未必需要选择 SCSI 硬盘，RAID 技术可以更加有效地提高磁盘的传输速度。

（3）SCSI 硬盘 CPU 占用率低、并行处理能力强。虽然 ATA/SATA 硬盘也能实现多用户同时存取，但当并行处理人数超过一定数量后，ATA/SATA 硬盘就会暴露出很大的 I/O 缺陷，传输速率有大幅下降。同时，硬盘磁头的来回摆动，也会造成硬盘发热性能不稳定。

对于 SCSI 而言，它有独立的芯片负责数据处理，当 CPU 将指令传输给 SCSI 后，随即去处理后续指令，其他的相关工作就交给 SCSI 控制芯片来处理。当 SCSI“处理器”处理完毕后，再次发送控制信息给 CPU，CPU 再接着进行后续工作，因此 SCSI 系统对 CPU 的占用率很低，而且 SCSI 硬盘允许一个用户对其进行数据传输的同时，另一位用户同时对其进行数据查找，这是 SCSI 硬盘并行处理能力的体现。

SCSI 硬盘较贵，但其品质性能更高，其独特的技术优势保障 SCSI 一直在中端存储市场占据主导地位。普通的 ATA 硬盘转速是 5400 或者 7200 RPM；SCSI 硬盘是 10k 或者 15k RPM，SCSI 硬盘的平均无故障时间达到 1 200 000 小时。另外，下一代 SCSI 技术 SAS 的诞生，则更好地兼容了性能和价格双重优势。

早期因为 SCSI 接口卡和设备昂贵，并且几乎各种外设都有较便宜的接口可替代，SCSI 并未受到青睐，可用的 SCSI 设备不多。反观今天，支持 SCSI 接口的外设产品从原本仅有硬盘、磁带机两种，增加到扫描仪、光驱、刻录机和 MO 等各种设备。再加上制造技术的进步，SCSI 卡与外设的价格下降幅度较大，显示 SCSI 市场已经相当成熟。

3．SCSI 控制卡

SCSI 卡是一种提供一个或一个以上（一个接口通过电缆可连接 15 个 SCSI 设备）的 SCSI 接口内置板卡，它可插在服务器（或其他设备）主板上的普通 PCI（或服务器上的 PCI-X）插槽上，实现多个 SCSI 接口的提供，以方便多个 SCSI 外设的连接。SCSI 控制器接口通常有 50 针、68 针和 80 针之分，常用的是 50 针和 68 针。SCSI 卡的出现解决了如下两方面的问题。

（1）使原来在主板中没有提供 SCSI 接口的服务器（或 PC）通过普通的 PCI 插槽连接 SCSI 接口的硬盘或其他外设。

（2）扩展了 SCSI 接口数量。

3.2.2　独立磁盘冗余阵列

1．磁盘阵列的特点

RAID（Redundant Array of Independent Disks，独立磁盘冗余阵列）有时也简称磁盘阵列（disk array）。磁盘阵列是由一个硬盘控制器来控制多个硬盘的相互连接，使多个硬盘的读写同步，减少错误，增加效率和可靠度的技术。而把这种技术加以实现的就是磁盘阵列产品，通常的物理形式就是一个长方体内容纳了若干个硬盘等设备，以一定的组织形式提供不同级别的服务。

简单地说，RAID 是一种把多块独立的硬盘（物理硬盘）按不同的方式组合起来形成一个硬盘组（逻辑硬盘），从而提供比单个硬盘更高的存储性能和提供数据备份技术。组成磁盘阵列的不同方式称为 RAID 级别（RAID Levels）。数据备份的功能是在用户数据一旦发生损坏后，利用备份信息可以使损坏数据得以恢复，从而保障了用户数据的安全性。在用户看来，组成的磁盘组就像是一个硬盘，用户可以对它进行分区、格式化等。总之，对磁盘阵列的操作与单个硬盘一样。不同的是，磁盘阵列的存储速度要比单个硬盘高很多，而且可以提供自动数据备份。

RAID 技术的两大特点：一是速度；二是安全。由于这两项优点，RAID 技术早期被应用于高级服务器中 SCSI 接口的硬盘系统中，随着近年计算机技术的发展，PC 的 CPU 速度已进入 GHz 时代。IDE 接口的硬盘也不甘落后，相继推出了 ATA66 和 ATA100 硬盘。这就使得 RAID 技术被应用于中低档甚至 PC 上成为可能。RAID 通常是由在硬盘阵列塔中的 RAID 控制器或计算机中的 RAID 卡来实现的。

2．RAID 技术分类

磁盘阵列分为全软阵列（software raid）、半软半硬阵列和全硬阵列（hardware raid）

三种。

（1）全软阵列。就是指 RAID 的所有功能都是由操作系统与 CPU 来完成，没有第三方的控制/处理芯片，即业界称其为 RAID 协处理器（RAID Co-Processor）与 I/O 处理芯片。这样，有关 RAID 的所有任务的处理都由 CPU 来完成。显而易见，这是一种低效的 RAID。

（2）半软半硬阵列。该阵列主要缺乏自己的 I/O 处理芯片，所以这方面的工作仍要由 CPU 和驱动程序来完成。而且，这种阵列所采用的 RAID 控制/处理芯片的能力一般都较弱，不能支持高的 RAID 等级。

（3）全硬阵列。该阵列全面具备了自己的 RAID 控制/处理芯片和 I/O 处理芯片，甚至还有阵列缓存（array buffer）。由于全硬阵列是一个完整的系统，所有需要的功能均可以做进去。所以，硬阵列所提供的功能和性能均比软阵列好。全硬阵列主要有两种方式，第一种就是 RAID 适配卡，通过 RAID 适配卡插入 PCI 插槽再接上硬盘实现硬盘的 RAID 功能。第二种方式就是直接在主板上集成 RAID 控制/处理芯片，让主板能直接实现磁盘 RAID。这种方式成本低于专用的 RAID 适配卡。表 3-2 是典型的软阵列和硬阵列性能参数的比较。

表 3-2　软阵列和硬阵列的比较

功　能	软　阵　列	硬　阵　列
数据完整性	探测 1 位错误（标准 SCSI 总线）	探测 4 位错误 修正 1 位错误
Raid 等级	Raid 0　和　Raid 1	基本上与操作系统无关，至于 RAID 等级要看厂商提供相应硬件功能、驱动和应用软件
热备用及自动化恢复	不可以	可以，专门的全程备用设计
重建优先级	不可以	低/中/高
可启动阵列	不可以	可以
错误报告	SNMP 过滤硬盘事件，用通用的系统标志报告	SNMP 用通用的系统标志报告，同时采用彩色代码发出警告和 E-mail 通告
预防性维护	不可以	对服务器、网络、无 RAID 存储空间进行轮流检测，安排阵列校验。对备用硬盘测试、磁盘重建
硬盘 SMART 技术支持	可以	可以
操作系统支持	一般 Windows 2k/XP 或 Linux	几乎所有的操作系统
性能	低	高
成本	低	较高

3．RAID 的基本工作模式

RAID 技术经过不断的发展，现在已拥有了从 RAID 0 到 6 这 7 种基本的 RAID 级别。另外，还有一些基本 RAID 级别的组合形式，如 RAID 10（RAID 0 与 RAID 1 的组合）、RAID 50（RAID 0 与 RAID 5 的组合）等。不同 RAID 级别代表着不同的存储性能、数据安全性和存储成本。最为常用的是下面的几种 RAID 形式。

1）RAID 0

RAID 0 又称为 Stripe（条带化）或 Striping，它代表了所有 RAID 级别中最高的存储性能。RAID 0 提高存储性能的原理是把连续的数据分散到多个磁盘上存取，这样，系统有数据请求就可以被多个磁盘并行地执行，每个磁盘执行属于它自己的那部分数据请求。这种数据上的并行操作可以充分利用总线的带宽，显著提高磁盘整体存取性能。

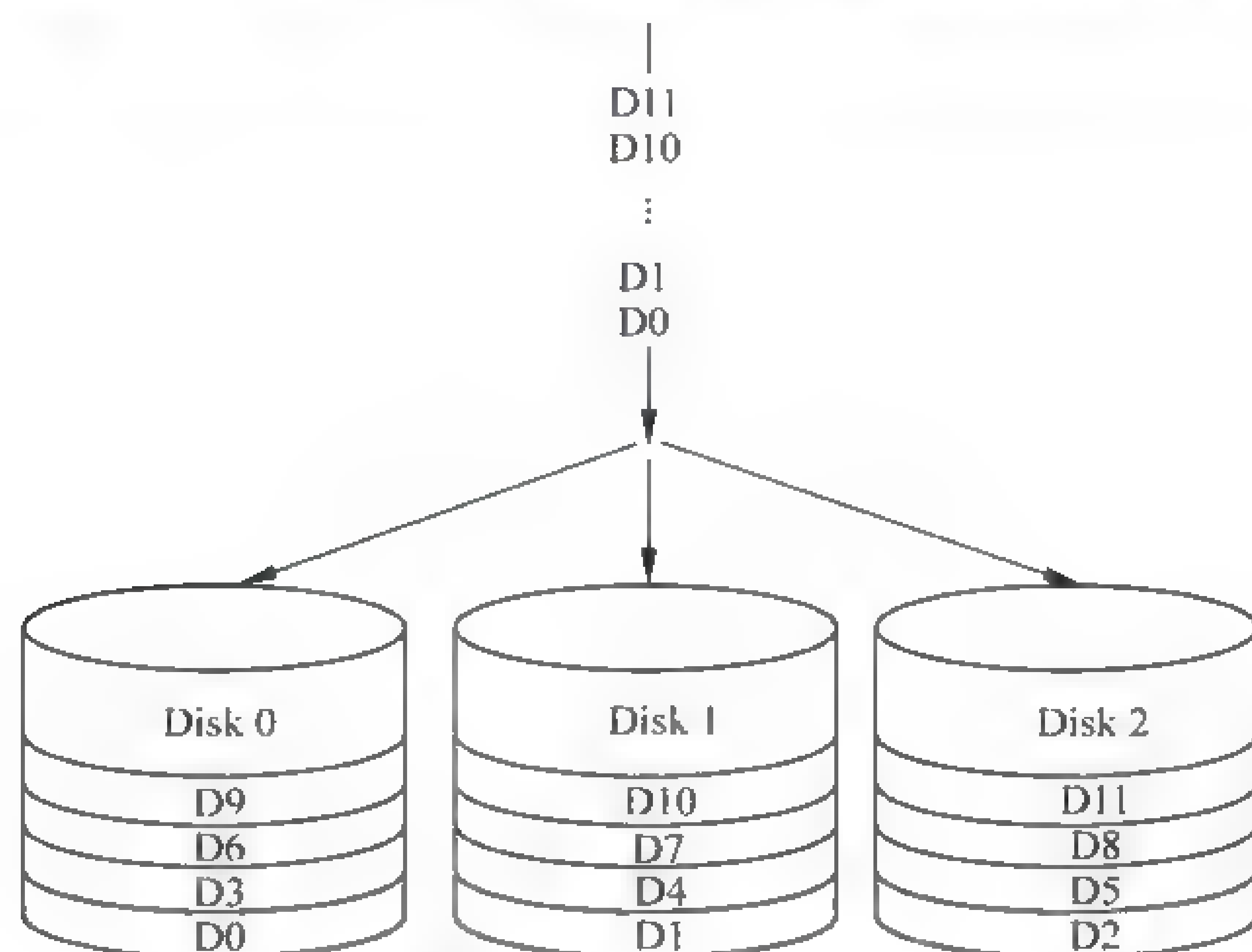


图 3-1　RAID 0 原理图

如图 3-1 所示，系统向三个磁盘组成的逻辑硬盘（RAID 0 磁盘组）发出的 I/O 数据请求被转化为三项操作，其中的每一项操作都对应于一块物理硬盘。从图中可以清楚地看到，通过建立 RAID 0，原先顺序的数据请求被分散到所有的三块硬盘中同时执行。从理论上讲，三块硬盘的并行操作使同一时间内磁盘读写速度提升了 3 倍。但由于总线带宽等多种因素的影响，实际的提升速率肯定会低于理论值，但是，大量数据并行传输与串行传输比较，提速效果显著显然毋庸置疑。

RAID 0 的缺点是不提供数据冗余，因此一旦数据损坏，损坏的数据将无法得到恢复。RAID 0 具有的特点，使其特别适用于对性能要求较高，而对数据安全要求低的领域，如图形工作站等。对于个人用户，RAID 0 也是提高硬盘存储性能的绝佳选择。

2）RAID 1

RAID 1 又称为 Mirror 或 Mirroring（镜像），它的宗旨是最大限度地保证用户数据的

可用性和可修复性。RAID 1 的操作方式是把用户写入硬盘的数据百分之百地自动复制到另外一个硬盘上。

如图 3-2 所示，当读取数据时，系统先从 RAID 0 的源盘读取数据，如果读取数据成功，则系统不去管备份盘上的数据；如果读取源盘数据失败，则系统自动转而读取备份盘上的数据，不会造成用户工作任务的中断。当然，应当及时地更换损坏的硬盘并利用备份数据重新建立 Mirror，避免备份盘在发生损坏时造成不可挽回的数据损失。

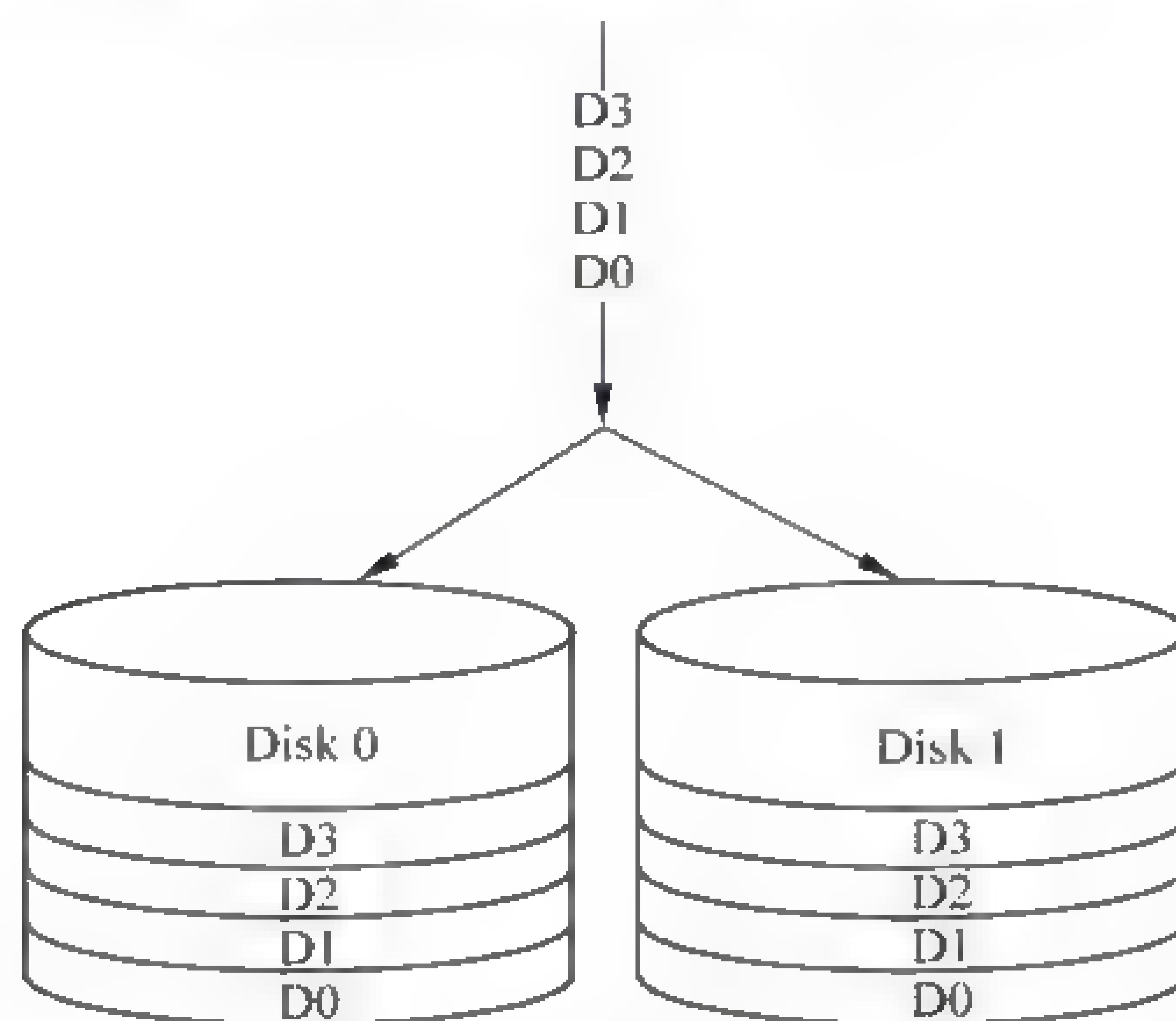


图 3-2 RAID 1 原理图

由于对存储的数据进行完全的备份，在所有 RAID 级别中，RAID 1 提供最高的数据安全保障。同样，由于数据的完全备份，备份数据占了总存储空间的一半，因而 Mirror 的磁盘空间利用率低，存储成本高。

Mirror 虽不能提高存储性能，但由于其具有的高数据安全性，使其尤其适用于存放重要数据，如服务器和数据库存储等领域。

3）RAID 3

RAID 3 是把数据分成多个“块”，按照一定的容错算法存放在 N+1 个硬盘上，实际数据占用的有效空间为 N 个硬盘的空间总和，而第 N+1 个硬盘上存储的数据是校验容错信息，当这 N+1 个硬盘中的一个硬盘出现故障时，从其他 N 个硬盘中的数据也可以恢复原始数据。这样，仅使用这 N 个硬盘也可以带伤继续工作（如采集和回放素材），当更换一个新硬盘后，系统可以重新恢复完整的校验容错信息。由于在一个硬盘阵列中，多于一个硬盘同时出现故障率的几率很小，所以一般情况下，使用 RAID 3，安全性是可以得到保障的。与 RAID 0 相比，RAID 3 在读写速度方面相对较慢。使用的容错算法和分块大小决定 RAID 使用的应用场合，在通常情况下，RAID 3 比较适合大文件类型且安全性要求较高的应用，如视频编辑、硬盘播出机和大型数据库等，如图 3-3 所示。

4）RAID 5

RAID 5 是一种存储性能、数据安全和存储成本兼顾的存储解决方案。以 4 个硬盘组

成的 RAID 5 为例，其数据存储方式如图 3-4 所示。图中，P0 为 D0、D1 和 D2 的奇偶校验信息，其他依此类推。从图中可以看出，RAID 5 不对存储的数据进行备份，而是把数据和相对应的奇偶校验信息存储到组成 RAID 5 的各个磁盘上，并且奇偶校验信息和相对应的数据分别存储于不同的磁盘上。当 RAID 5 的一个磁盘数据发生损坏后，利用剩下的数据和相应的奇偶校验信息去恢复被损坏的数据。

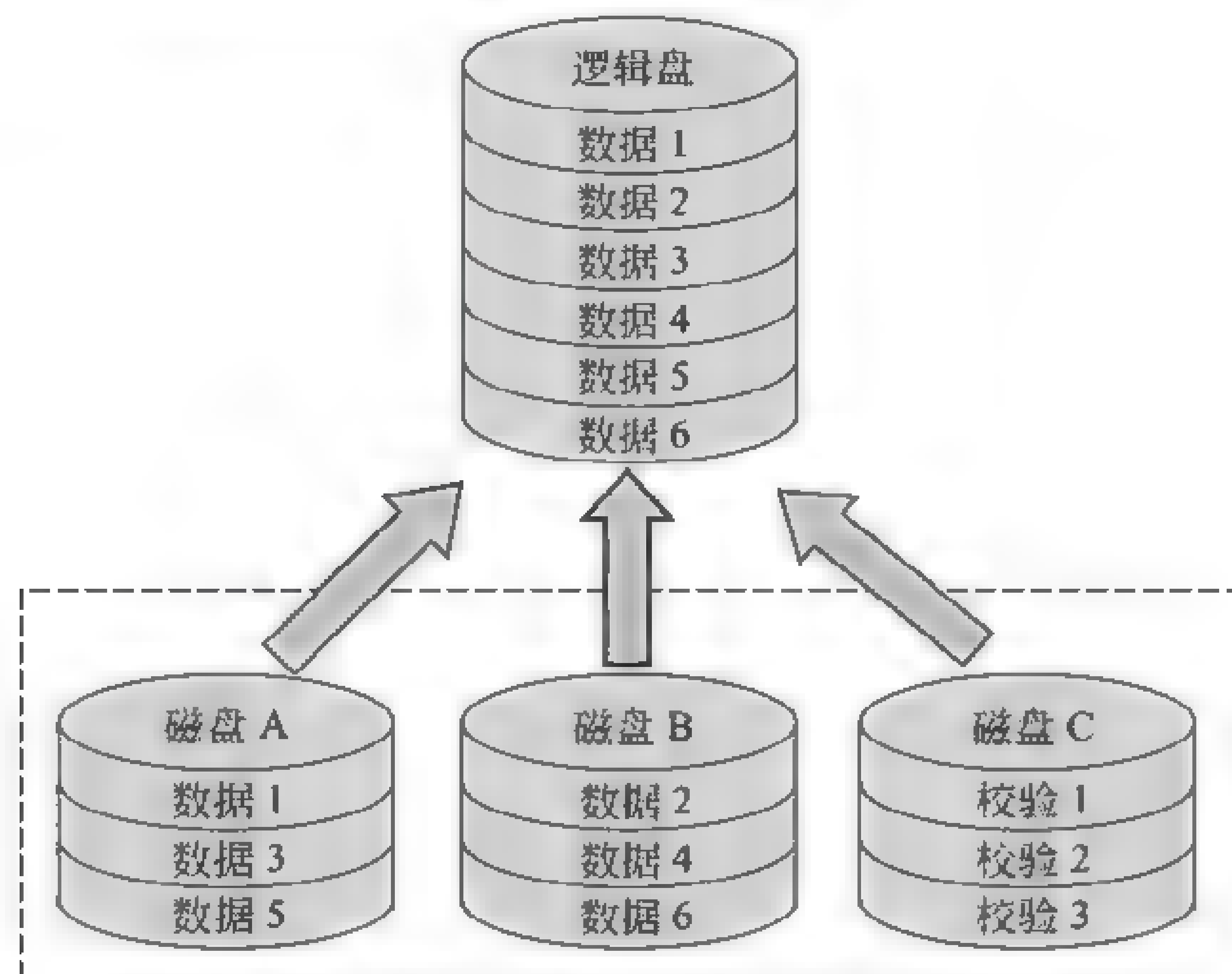


图 3-3　RAID 3 原理图

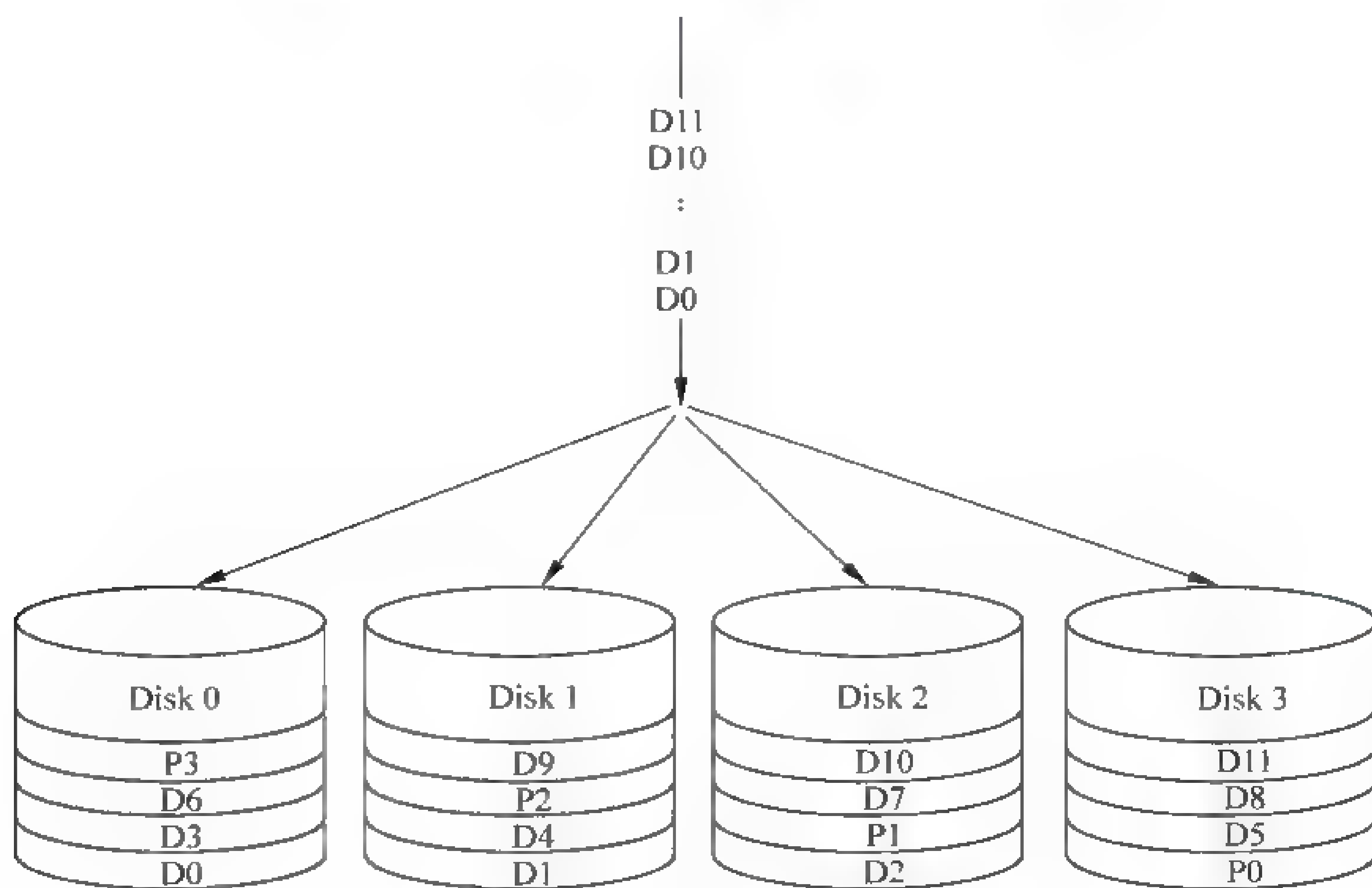


图 3-4　RAID 5 原理图

RAID 5 可以理解为是 RAID 0 和 RAID 1 的折衷方案。RAID 5 可以为系统提供数据安全保障，但保障程度要比 Mirror 低而磁盘空间利用率要比 Mirror 高。RAID 5 具有和 RAID 0 相近似的数据读取速度，只是多了一个奇偶校验信息，写入数据的速度比对单个磁盘进行写入操作稍慢。同时，由于多个数据对应一个奇偶校验信息，RAID 5 的磁盘空间利用率要比 RAID 1 高，存储成本相对较低。

5）RAID 0+1

正如其名字一样，RAID 0+1 是 RAID 0 和 RAID 1 的组合形式，也称为 RAID 10。以 4 个磁盘组成的 RAID 0+1 为例，其数据存储方式如图 3-5 所示。RAID 0+1 是存储性能和数据安全兼顾的方案，它在提供与 RAID 1 一样的数据安全保障的同时，也提供了与 RAID 0 近似的存储性能。

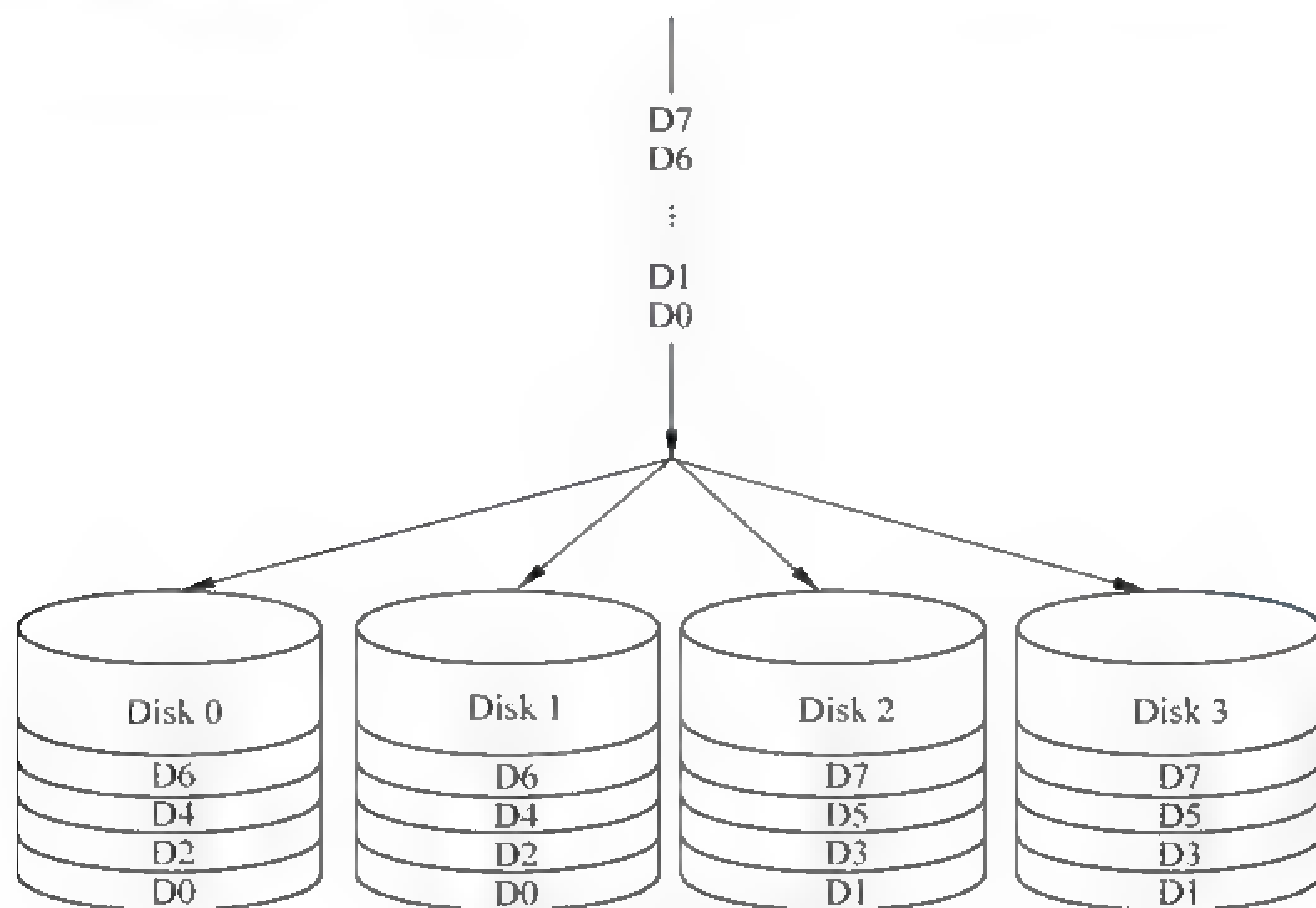


图 3-5 RAID 0+1 原理图

由于 RAID 0+1 也通过数据的 100%备份功能提供数据安全保障，因此 RAID 0+1 的磁盘空间利用率与 RAID 1 相同，存储成本高。RAID 0+1 的特点使其特别适用于既有大量数据需要存取，同时又对数据安全性要求严格的领域，如银行、金融、商业超市、仓储库房和各种档案管理等。

4．RAID 级别的选择

RAID 级别的选择有三个主要因素：可用性（数据冗余）、性能和成本。如果不要求可用性，选择 RAID 0 以获得最佳性能。如果可用性和性能是重要的而成本不是一个主要因素，则根据硬盘数量选择 RAID 1。如果可用性、成本和性能都同样重要，则根据一般的数据传输和硬盘的数量选择 RAID 3 或 RAID 5。关于 RAID 级别的描述，请见表 3-3。

表 3-3　RAID 级别性能比较

RAID 级别	RAID 0	RAID 1	RAID 3	RAID 5	RAID 10
别名	条带	镜像	专用奇偶位条带	分布奇偶位条带	镜像阵列条带
容错性	没有	有	有	有	有
冗余类型	没有	复制	奇偶校验	奇偶校验	复制
热备盘选项	没有	有	有	有	有
读性能	高	低	高	高	中间
随机写性能	高	低	最低	低	中间
连续写性能	高	低	低	低	中间
需要的磁盘数	1 个或多个	只需 2 个或 2N 个	3 个或更多	3 个或更多	只需 4 个或 2N 个
可用容量	总的磁盘容量	只能用磁盘容量的 50%	$(n-1)/n$ 的磁盘容量，其中 n 为磁盘数	$(n-1)/n$ 的磁盘容量，其中 n 为磁盘数	只能用磁盘容量的 50%
典型应用	无故障地迅速读写，要求安全性不高，如图形工作站等	随机数据写入，要求安全性高，如服务器、数据库存储领域	连续数据传输，要求安全性高，如视频编辑、大型数据库等	随机数据传输，要求安全性高，如金融、数据库和存储等	要求数据量大，安全性高，如银行、金融等领域

3.2.3　磁带库

1．备份设备类型

在选择备份设备时，根据备份数据量的大小、对备份速度的要求、对自动化程度的要求等，用户可以选择不同档次的设备。备份设备主要分为磁带机、自动加载机和磁带库，而磁带库又分为入门级、企业级和超大容量等几个级别。

磁带机又称磁带驱动器，简称带机，是读写磁带的基本设备。它通过 SCSI 线缆与服务器直连，相当于服务器的外设，分为内置和外置两种。一台带机一次只能容纳一盘磁带，需要人工换带，自动化程度低。一般只用于单台服务器备份，适合于数据量非常小的企业。

如果企业希望通过预先制定的备份策略，实现备份过程和备份介质的自动化管理，减少系统管理的工作量，则需要购买能够容纳多盘磁带的设备，即自动加载机或带库。自动加载机内一般能够容纳 4～20 盘磁带。它与带库的主要区别在于不是通过机械手抓取磁带，而是通过一个简单的自动传送装置移动磁带，并且只能配一台磁带驱动器。因此实现成本较低，但功能也受到限制。它虽然能够支持自动备份，但仍然属于低端的备份设备，适合于单台服务器或小型网络。

磁带库（简称带库）是专业的备份设备，它主要由库体、磁带驱动器、磁带槽位、磁带交换口、控制面板、机械手和电子控制单元组成。库体内的大部分空间用于放置磁带，一台或多台驱动器安装在库体内专门的位置，用于读写磁带。带库工作时，机械手在管理软件和电子控制单元的控制下移动，通过安装在机械臂上的条码读取器寻找相应的磁带，然后将其抓取到驱动器内；读或写操作完成后，再由机械手将磁带取出，放回磁带槽位。

由于带库内可安装多个驱动器，因此能够支持并发的多任务；对于一个大的备份任务，也可以分配到多个驱动器上并行读/写，从而大大提高备份效率，有效地缩小备份窗口。当然，这些功能需要备份管理软件的支持。

一般具有几十个磁带槽位的带库属于入门级，几百个槽位的属于企业级，几千个槽位的则属于超大容量带库。企业级以上的带库还支持一些复杂的功能，如分区管理、磁带混装和级联扩展等。另外，随着 SAN 技术和 LAN-free 备份方式的推广，越来越多的企业将带库连接到 SAN 上作为共享的存储资源。因此，带库厂商也非常重视带库对 SAN 的支持，很多企业级带库不仅提供光纤通道接口，还增加了 SAN 环境下的管理功能。

2. 磁带驱动技术

磁带驱动技术是指磁带驱动器遵循的标准，它规定了数据格式、记录方式、定位方式、走带路径、校验方式、压缩算法、介质尺寸、介质生产工艺以及驱动器的接口标准等。在驱动器和磁带的生产过程中，都必须遵从某一种驱动技术的标准。只有采用相同标准生产出来的驱动器和磁带才能一起工作。

每个磁带驱动器都对应着某种特定的磁带驱动技术，例如，Sony AIT 磁带机采用的就是 AIT 技术，而 Quantum 的 DLT 磁带机采用的是 DLT 技术。但是，磁带库本身与磁带驱动技术则没有任何必然的联系，也就是说一台带库可以支持多种不同的磁带驱动器，甚至可以支持混装。带库能够支持多少种驱动技术，反映了它的开放性。一般来说，企业信息系统都非常注重开放性，防止在系统扩展时受到某种技术和产品的限制。但是在一些特殊领域，则可能由于行业特点或行业习惯一直沿用某种产品，而不是非常重视开放性。

目前主流的磁带驱动技术包括 Quantum 公司的 DLT 和 SuperDLT，IBM、HP 和 Seagate 共同制定的 LTO，STK 的 9840、9940，IBM 的 3590，Exabyte 的 Mammoth-2，Sony 的 AIT-2、AIT-3、DTF、DTF-2 等。

磁带驱动技术最主要的指标是数据传输率和单盘容量，因为这直接关系到做一次备份所需的时间和介质数量。查看这两个指标时要注意区分厂家给出的数值是未压缩模式下的，还是在 2∶1 或更高压缩比下的。另外，还要注意区分峰值数据传输率和持续数据传输率的不同，峰值传输率是指瞬间可达的最大传输率，它不能反映带机的整体性能，用户真正应该关心的是持续传输率。反映带机性能的另一个指标是载入时间，是指将一盘磁带插入带机、至带机准备好、再到可进行读写操作所需的时间，一般为几秒到几十

秒。相对于备份任务所需的全部时间，载入时间是非常微不足道的。但当带库用于数据迁移（storage migration）系统时，由于需要频繁交换磁带，带机的载入时间长短就比较重要了。

除了容量和性能外，一般用户比较关心的要算可靠性了，特别是对那些需要带机高负荷工作的系统，可靠性就更为重要。衡量可靠性的一个最常用指标是 MTBF（平均无故障时间），它是指带机在出现故障之前平均的正常工作时间。这一指标并不是通过实测得到的，而是综合了影响带机运作的各种因素，以一定的公式计算得出。目前主流的驱动技术其 MTBF 都可达到十几万到几十万小时。带机内部的稳定性，与磁头设计、走带路径造成的张力和磨损等因素有关。表 3-4 简单对比了几种主流磁带驱动技术。

表 3-4　主流磁带驱动技术指标

	单盘容量（GB）	持续传输率(MBps)	记录方式	介质类型	介质寿命（年）
LTO	100	15	线形	MP	30
SuperDLT	110	11	线形	AMP	>30
9940	60	10	线形	AMP	15～30
3590	20/40/60	14	线形	AMP	15～30
AIT-3	100	12	螺旋扫描	AME	>30
DTF-2	200/60	24	螺旋扫描	AMP	>30
Mammoth-2	60	12	螺旋扫描	AME	30

3．带机、带库厂商及产品

备份设备的生产厂家很多，每个厂家都有着较长的产品线。这里主要介绍那些国际知名的、国内有影响力的带机和带库厂商及其主打产品。

目前，带机正在朝快的数据传输速度和高的单盘磁带存储容量方向发展，具有主流驱动技术的带机厂商包括 Quantum、Exabyte 和 Sony 等。

Quantum 带机在中档产品中占据了市场大部分份额，但其中很大一部分走了 OEM 的销售渠道。其自动加载机 SuperLoader 可将多个备份目标集中到一个共享的自动系统中，降低处理成本，而基于磁盘（备份介质是磁盘）又具有磁带海量特性的近线备份设备 DX30 可显著缩短备份与恢复时间。

Exabyte 的磁带驱动技术包括 8mm Mammoth 和 VXA 技术，VXA 是定位低端的新的磁带技术，它以包的格式读写数据，并可对磁带上的数据记录区进行无空隙扫描，具有高质量、高可靠性、低成本等性能特点。其中，VXA-1 带机是专为苹果机设计的存储方案；VXA-2 同样具有较高的性价比，并具有 12MBps 的传输速率及 160GB 的容量，与 VXA-1 向下兼容。

Sony 的基于 AIT 技术的带机产品：AIT-1、AIT-2 和 AIT-3，其中 AIT-3 是高性能和大容量的新存储方案，容量（未压缩）为 100GB，速率为 12MBps，而且能够与 AIT-1、

AIT-2 完全读和写逆向兼容，并具有分层磁头、创新性的磁带内存储器（MIC）驱动器接口系统等多项专利技术，提高磁轨密度和存储速度。

磁带库厂商相对品牌较多，用户的选择空间也更大一些。目前主流的磁带库厂商主要有 STK、Quantum、Exabyte 和 IBM 等。

在带库厂商中，市场份额最大的当属 SUN 公司收购的美国存储技术公司（StorageTek，STK）。STK 目前最主要的产品线是 L 系列，包括 L20、L40、L80、L180、L700、L5500，从最小 20 磁带槽位到最大 5500 磁带槽位。在其入门级产品上，支持 LTO、DLT 和 SuperDLT 等开放技术，只有在高端产品上才同时支持其自身拥有的 9840、9940 驱动技术。

Quantum 拥有 DLT、SuperDLT 技术，其用户基础和发展前景都很好。其 P 系列的主打产品 P4000 和 P7000 分别可以支持几百槽位和十几个驱动器，适合于企业级用户；M 系列是模块化的产品，可根据用户系统需求的增长灵活扩展带库的容量和性能，M1500 可从 20 槽位扩展到 200 槽位，M2500 则可从 100 槽位扩展到 300 槽位，非常适合于那些快速发展的中小企业。美中不足的是，ATL 对超大容量的解决方案不是非常理想，在这一部分市场上的竞争力较弱。

8mm 是安百特（Exabyte）公司的独立技术，具有速度快、容量大、可靠性高、价廉、体积小等特点，主要用于带库，其 8mm 带库的智能机械臂系统可任意存取磁带，采用模块化设计，产品线全，从 VXA 自动化/驱动器产品系列 AutoPak230/115/110、VXA-1/1 到 Mammoth Tape 自动化/驱动器产品系列 X200/80/430M/215M/EZ17、M2/Mammoth/Eliant 820，容量从单盘（非压缩）33GB 到整库 12TB，涵盖由低到高的用户市场，可实现无人值守自动数据存储管理，适用于服务器备份、网络备份、自动归档、分级存储管理及图形图像等领域。

IBM 的带库和带机产品大体可分两个系列：用于 IBM 环境的和用于开放环境的。如 IBM 的 3494、3575 等带库只支持其专用的驱动器，开放性差，虽然这些带库产品也支持 HP、SUN 等主流服务器平台，但实际上几乎只用在 IBM 环境中。随着 SAN 技术的普及，追求开放性和互联性成为存储行业的潮流。结合 LTO 驱动技术的投产，IBM 为其开放存储系统解决方案推出了新的带库系列 3583 和 3584。表 3-5 列出了上述带库生产厂家部分产品的参数。

表 3-5 主流带库产品参数表

厂家	产品型号	磁带槽位	最大驱动器数	驱动技术类型	是否可级联
STK	L20	10、20	2	DLT8000 SDLT LTO Ultrium 9840、9940	否
	L40	20、40	4		否
	L80	40、60、80	8		否
	L180	174	10		否
	L700	678、1344	24、40		是
	L5500	5500（单台）	80		是

续表

厂　家	产品型号	磁带槽位	最大驱动器数	驱动技术类型	是否可级联
Quantum	M1500	20～200（10 模块）	20	DLT8000 SDLT LTO Ultrium	是
	M2500	100～300（3 模块）	18		是
	P4000	171～322（单台）	10		是
	P7000	399～679（单台）	16		是
IBM	3583	72	6	LTO Ultrium	否
	3584	2481（6 模块）	72		是
	3494	160～6240	32	3490e、3590	是
Exabyte	X200 X80 430M 215M	200 80 30 15	10 8 4 2	Mammoth-2、 Mammoth Mammoth-2、 Mammoth Mammoth Mammoth-2	

4．产品选购指南

当真的准备建设备份系统、购买备份设备时，需要考虑和考查哪些问题呢？

首先，要选择符合应用特点的驱动技术。前面已经介绍过比较驱动技术时主要考虑哪些方面，但事实上每种技术都有它的特点和优点，不是通过简单的参数对比就能比出高下的。真正需要采购时还是要结合实际需求，根据应用特点确定驱动技术的哪一项或哪几项指标比较重要。例如，对于备份和归档的数据量非常大的应用系统而言，选用单盘容量大的磁带驱动技术，从长远角度看是可以有效降低介质成本和管理成本的；而对于需要时常访问归档数据的信息系统，则应注重驱动器的载入时间和读写速度，从而有效降低用户的等待时间。另外，在考虑驱动技术自身特性的同时，要考虑其成熟性和发展性。

选定驱动技术之后，就可以根据需要备份的数据量、信息系统对备份窗口的要求以及采用何种备份策略等因素，确定所需带库的容量和备份速度，从而基本确定可供选择产品的范围。从备选产品中进行第二轮筛选，则要具体分析每个产品的功能和特点，看它是否具备某项需要的功能，是否有某项缺点恰好影响使用。例如，某大型企业网上运行着多个应用系统，希望做集中的数据存储和数据备份，由于应用和数据类型的多样化，可能需要采用不同的磁带格式进行备份，这时带库的分区管理功能和对混合介质的管理功能就是必不可少的。

筛选过后留下的产品基本都能满足需要，这时当然取决于性价比了。不过，在最后选定一款产品前，一定记得请厂家或代理商核查兼容性列表，特别是用户的信息系统环境比较复杂时，要确认该产品与原有的，以及计划增加的设备及软件的兼容性。这个环

节非常重要，因为带库不是独立工作的，而是与备份服务器、备份客户端、备份管理软件共同组成备份系统。如果忽视了这个环节，可能会给系统实施带来严重的问题。

在带库的选择过程中，不要忘记考虑未来的扩展需求。信息系统是不断发展的，基础设施的建设也不可能一步到位。如果在设计初期考虑到带库的扩容能力和功能的多样性，就可以从容面对信息系统需求的发展和变化。

5. 虚拟磁带库

虚拟磁带库（Virtual Tape Library，VTL）是使用磁盘阵列效仿标准磁带库的一种新概念产品。VTL 通过光纤连接到备份服务器，为数据存储备份提供了高速、高效及安全的解决方案，极大地缩短了数据备份所需时间。更重要的是，VTL 通过冗余和热插拔设计保证了系统的不停顿及备份工作连续运行。

从目前中国存储市场的现状看，大多数用户仍使用磁带承担备份和归档的双重任务，究其原因，是因为磁带远比磁盘价廉。但在使用常规磁带库时经常会被下列问题困扰。

（1）机械手、驱动器、磁带多个暴露机械装置中任一单点故障，均会导致备份失败。

（2）备份磁带组中任一盘磨损、卡带、变形、受潮等，均可能导致整体备份无法恢复。

（3）耗时的文件查找，困扰日常运营，严重制约 IT 服务能力。

随着 ATA、SATA 磁盘阵列的出现，并且 ATA、SATA 磁盘的成本正逐渐接近甚至低于磁带，基于磁盘的备份技术正在成为一种潮流，磁盘有取代磁带成为备份主流介质的趋势。虽然 VTL 问世的时间不长，但在国外却是相当热门的产品，从市场面来看，主要的储存设备供货商都开始开发 VTL 产品线。

3.2.4 光盘塔

光盘塔由几台或十几台 CD-ROM 驱动器并联构成，可通过软件控制某台光驱的读写操作。光盘塔可以同时支持几十个到几百个用户访问信息。

光盘库实际上是一种可存放几十张或几百张光盘并带有机械臂和一个光盘驱动器的光盘柜。光盘库也叫自动换盘机，它利用机械手从机柜中选出一张光盘送到驱动器进行读写。它的库容量极大，机柜中可放几十片甚至上百片光盘片，这种有巨大联机容量的设备非常适用于图书馆一类的信息检索中心，尤其是交互式光盘系统、数字化图书馆系统、实时资料档案中心系统及卡拉 OK 自动点播系统等。

光盘网络镜像服务器是继第一代的光盘库和第二代的光盘塔之后，最新开发出的一种可在网络上实现光盘信息共享的网络存储设备。光盘网络镜像服务器不仅具有大型光盘库的超大存储容量，而且还具有与硬盘相同的访问速度，其单位存储成本大大低于光盘库和光盘塔。代表产品有清华同方光盘镜像服务器。

在网络海量存储备份系统中，磁盘阵列、磁带库和光盘库等存储设备因其信息存储特点的不同，应用环境也有较大区别。磁盘阵列主要用于网络系统中的海量数据的即时

存取；磁带库更多的是用于网络系统中的海量数据的定期备份；光盘库则主要用于网络系统中的海量数据的访问。光盘库的优点是能按需求保存数据，且保存的数据具可移动性。缺点是光盘容量非常有限及购买光盘的花费大，刻录机寿命不长，人工操作，而且光盘易丢失损坏。

3.2.5　DAS 技术

DAS（Direct Attached Storage，直接附加存储）即直连方式存储。在这种方式中，存储设备是通过电缆（通常是 SCSI 接口电缆）直接连接服务器。I/O（输入输出）请求直接发送到存储设备。DAS 也可称为 SAS（Server-Attached Storage，服务器附加存储）。它依赖于服务器，其本身是硬件的堆叠，不带有任何存储操作系统。图 3-6 为典型的 DAS 结构图。

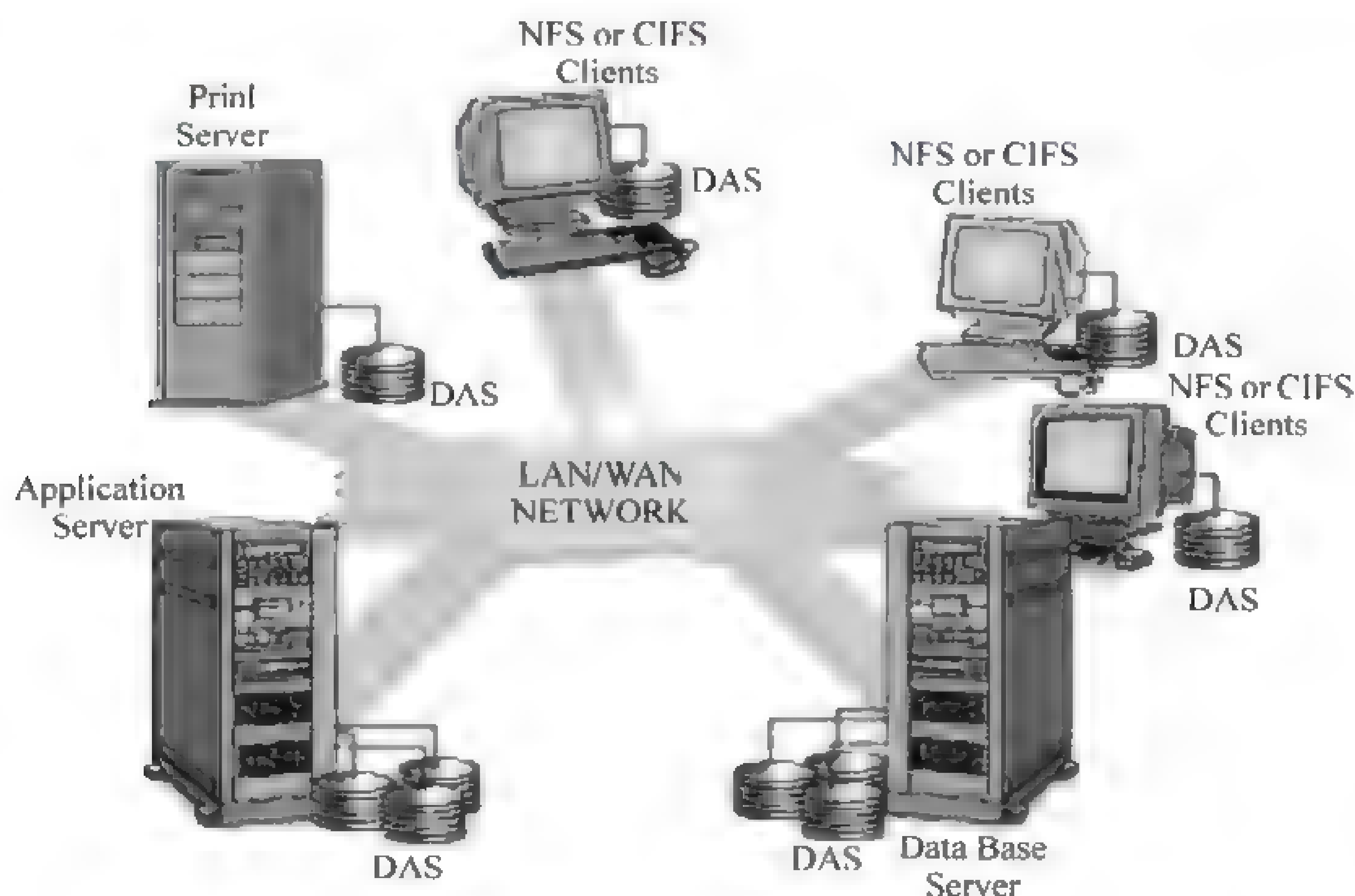


图 3-6　典型的 DAS 结构

DAS 的适用环境如下。

（1）服务器在地理分布上很分散，通过 SAN（存储区域网络）或 NAS（网络直接存储）在它们之间进行互连非常困难时。

（2）存储系统必须被直接连接到应用服务器（如 Microsoft Cluster Server 或某些数据库使用的“原始分区”）上时。

（3）包括许多数据库应用和应用服务器在内的应用，它们需要直接连接到存储器上时。

对于多个服务器或多台 PC 的环境，使用 DAS 方式设备的初始费用可能比较低，可是这种连接方式下，每台 PC 或服务器单独拥有自己的存储磁盘，容量的再分配困难；

对于整个环境下的存储系统管理，工作烦琐而重复，没有集中管理解决方案。所以，整体的拥有成本（TCO）较高。目前，DAS 基本被 NAS 所代替。

3.2.6 NAS 技术

在 NAS（Network Attached Storage，网络附加存储）结构中，存储系统不再通过 I/O 总线附属于某个特定的服务器或客户机，而是直接通过网络接口与网络相连，由用户通过网络来访问。NAS 与 DAS 的比较如表 3-6 所示。

NAS 实际上是一个带有瘦服务的存储设备，其作用类似于一个专用的文件服务器，不过把显示器、键盘和鼠标等设备省去。NAS 用于存储服务，可以大大降低存储设备的成本。另外，NAS 中的存储信息都是采用 RAID 方式进行管理的，从而有效地保护了数据。

在访问资源方面也非常方便，用户访问 NAS 同访问一台普通计算机的硬盘资源一样简单，甚至可以设置 NAS 设备为一台 FTP 服务器，这样其他用户就可以通过 FTP 访问 NAS 中的资源了。在管理方面也可以通过网页浏览的方式进行管理。

表 3-6　NAS 与 DAS 的比较

比较项目	NAS	DAS
核心技术	基于 Web 开发的软硬件集合于一身的 IP 技术，部分 NAS 是软件实现 RAID 技术	硬件实现 RAID 技术
支持操作平台	完全跨平台文件共享，支持所有的操作系统	不能提供跨平台文件共享功能，受限于某个独立的操作系统
连接方式	通过 RJ45 接口连上网络，直接往网络上传输数据，可接 10M/100M/1000M 网络	通过 SCSI 线接在服务器上，通过服务器的网卡往网络上传输数据
安装	安装简便快捷，即插即用	通过 LCD 面板设置 RAID 较简单，连上服务器操作时较复杂
操作系统	独立的 Web 优化存储操作系统，完全不受服务器干预	无独立的存储操作系统，需相应服务器的操作系统支持
存储数据结构	集中式数据存储模式，将不同系统平台下文件存储在一台 NAS 设备上，方便网络管理员集中管理大量的数据，降低维护成本	分散式数据存储模式，网络管理员需要耗费大量时间到不同服务器下分别管理各自的数据，维护成本增加
数据管理	管理简单，基于 Web 的 GUI 管理界面使 NAS 设备的管理一目了然	管理较复杂，需要服务器附带的操作系统支持
软件功能	自身支持多种协议的管理软件，功能多样，支持日志文件系统，并一般集成本地备份软件	没有自身管理软件，需要针对现有系统情况另行购买

续表

比 较 项 目	NAS	DAS
扩充性	轻松在线增加设备，无须停顿网络，而且与已建立起的网络完全融合，充分保护用户原有投资，良好的扩充性完全满足 24×7 不间断服务	增加硬盘后重新做 RAID 一般要停机，会影响网络服务
总拥有成本	价格低，不需要购买服务器及第三方软件，以后的投入会很少，降低用户的后续成本，从而使总拥有成本降低	价格较适中，需要购买服务器及操作系统，总拥有成本较高
数据备份与灾难恢复	集成本地备份软件，可实现无服务器的网络数据备份。双引擎设计理念，即使服务器发生故障，用户仍可进行数据存取	可备份直连服务器及工作站的数据，对多个服务器的数据备份较难
RAID 级别	RAID0、1、5 或 JBOD	RAID0、1、3、5 或 JBOD
硬件架构	冗余电源、多风扇、热插拔	冗余电源、多风扇、热插拔、背叛化结构

3.2.7　SAN 技术

SAN 是通过专用高速网将一个或多个网络存储设备和服务器连接起来的专用存储系统，未来的信息存储将以 SAN 存储方式为主。SAN 主要采取数据块的方式进行数据和信息的存储，目前主要使用于以太网和光纤通道两类环境中。NAS 与 SAN 的比较如表 3-7 所示。

通过 IP 协议或以太网的数据存储，IP 存储使得性价比较好的 SAN 技术能应用到更广阔的市场中。它利用廉价、货源丰富的以太网交换机、集线器和线缆来实现低成本、低风险基于 IP 的 SAN 存储。

光纤通道是一种存储区域网络技术，它实现了主机互连，企业间共享存储系统的需求。可以为存储网络用户提供高速、高可靠性以及稳定安全性的传输。光纤通道是一种高性能、高成本的技术。

另外，无限带宽技术（infiniband）是一种高带宽、低延迟的下一代互连技术，构成新的网络环境，实现 IB SAN 的存储系统。

表 3-7　NAS 与 SAN 的比较

比 较 项 目	NAS	SAN
文件系统	基于 File system 的	基于 LUN 的
连接方式	连接在 LAN 中的存储服务器	由 FC 交换机组成的一个存储网络
操作系统	是和 Cluster 无关的，NAS 设备有自己的 OS	是和 Cluster 密切相关的，SAN 中的存储设备没有 OS

续表

比 较 项 目	NAS	SAN
存储数据结构	NAS 上的数据是不排外的，同一个逻辑区域可以被多个服务器读取和修改	SAN 上的数据是放在 LUN 上的，同一个区域需要 Lock Manager 来控制，不允许同时读写
体系结构	主要作为散布在 LAN 中的各个分开的存储系统	主要是作为一个整体概念存在于企业中，可以看作一个单独的存储系统
协议集	廉价的，走的是 TCP/IP	昂贵的，走的是 FC 相关协议集
总拥有成本	性能/价格比较好，适合中小企业的中央存储	性能优秀，但是价格昂贵，适合大型企业和关键应用的核心存储系统

1．FC SAN 技术

由于应用的不断要求，光纤通道技术已经确立成为 SAN 互连的精髓，可以为存储网络用户提供高速、高可靠性以及稳定安全性的传输。光纤通道技术是基于美国国家标准协会（ANSI）的 X3.230-1994 标准（ISO 14165-1），而创建的基于块的网络方式。该技术详细定义了在服务器、转换器和存储子系统（例如，磁盘列阵或磁带库）之间建立网络结构所需的连接和信号。光纤通道几乎可以传输任何大小的流量。

光纤通道采用光纤以 1Gbps、2Gbps、4Gbps 和最新的 10Gbps 速率传输 SAN 数据。同时，延迟时间短，尽量缩短数据请求和发送的迟缓时间。例如，典型的光纤通道转换所产生的延时仅有数微秒。正是由于光纤通道结合了高速度与延迟性低的特点，在时间敏感或交易处理的环境中，光纤通道成为理想的选择。同时，这些特点还支持强大的扩展能力，允许更多的存储系统和服务器互连。光纤通道同样支持多种拓扑结构，既可以在简单的点对点模式下实现两个设备之间的运行，也可以在经济型的仲裁环下连接 126 台设备，或者（最常见的情况）在强大的交换式结构下为数千台设备提供同步全速连接。

2．IP SAN 技术

1）IP SAN 概述

IP SAN 存储技术，顾名思义，是在传统 IP 以太网上架构一个 SAN 存储网络把服务器与存储设备连接起来的存储技术。IP SAN 其实是在 FC SAN 的基础上再进一步，它把 SCSI 协议完全封装在 IP 协议之中。简单来说，IP SAN 就是把 FC SAN 中光纤通道解决的问题通过更为成熟的以太网来实现。从逻辑上讲，它是彻底的 SAN 架构，即为服务器提供块级服务。

2）IP SAN 的特性

IP SAN 技术有其独特的优点：节约大量成本、加快实施速度、优化可靠性以及增强扩展能力等。采用 iSCSI 技术组成的 IP SAN 可以提供和传统 FC SAN 相媲美的存储解决方案，而且普通服务器或 PC 只需要具备网卡，即可共享和使用大容量的存储空间。与传统的分散式直连存储方式不同，它采用集中的存储方式，极大地提高了存储空间的

利用率，方便了用户的维护管理。

iSCSI 是基于 IP 协议的，它能容纳所有 IP 协议网络中的部件。通过 iSCSI，用户可以穿越标准的以太网线缆，在任何需要的地方创建实际的 SAN 网络，而不需要专门的光纤通道网络在服务器和存储设备之间传送数据。iSCSI 可以实现异地间的数据交换，使远程镜像和备份成为可能。因为没有光纤通道对传输距离的限制，IP SAN 使用标准的 TCP/IP 协议，数据即可在以太网上进行传输。

3）IP SAN 和 FC SAN 的比较

SAN 主要包含 FC SAN 和 IP SAN 两种，FC SAN 的网络介质为光纤通道（Fibre Channel），而 IP SAN 使用标准的以太网。采用 IP SAN 可以将 SAN 为服务器提供的共享特性以及 IP 网络的易用性很好地结合在一起，并且为用户提供了类似服务器本地存储的较高性能体验。SAN 是一种进行块级服务的存储架构，一直以来，光纤通道 SAN 发展相对迅速，因此，一度认为只能通过光纤通道来实现 SAN。然而，通过传统的以太网仍然可以构建 SAN，那就是 IP SAN。

iSCSI 是实现 IP SAN 最重要的技术。在 iSCSI 出现之前，IP 网络与块模式（主要是光纤通道）是两种完全不兼容的技术。由于 iSCSI 是运行在 TCP/IP 之上的块模式协议，它将 IP 网络与块模式的优势很好地结合起来，且 IP SAN 的成本低于 FC SAN。

4）IP SAN 解决方案

IP SAN 存储解决方案有着广泛的行业适用性，在备份和恢复、高可用性、业务连续性、服务器和存储设备整合等方面，采用 iSCSI 技术组成的 IP SAN 存储可与 FC SAN 相媲美。IP SAN 构建成本更低，而且可以连接更远的距离，对于电信、企业、教育、政府、专业设计公司、音/视频处理、新闻出版、ISP\ICP、科研院所和信息中心等行业用户都比较适用。



图 3-7　典型的 IP SAN 解决方案

图 3-7 为比较简单的 IP SAN 结构图。例子中使用千兆以太网交换机搭建网络环境，由非编制作工作站、文件服务器和磁盘阵列及磁带库组成。图中服务器、工作站使用 iSCSI HBA（Host Bus Adapter，主机总线适配卡）通过交换机连接。为强调 HBA 卡，特意另外画出标明。iSCSI HBA 包括网卡的功能，还支持 OSI 网络协议堆栈以实现协议转换的功能。

注意，如果不用 HBA 卡，也可以用软件实现 SCSI 协议和 TCP/IP 协议之间的转换。但这比较消耗 CPU 资源。如果采用软件，服务器配置建议采用双 CPU。在 IP SAN 中还可以将基于 iSCSI 技术的磁带库直接连接到交换机上，通过存储管理软件实现简单、快速的数据备份。

3．IB SAN 技术

1）IB SAN 概述

InfiniBand 是一种交换结构 I/O 技术，其设计思路是通过一套中心机构 InfiniBand 交换机在远程存储器、网络以及服务器等设备之间建立一个单一的连接链路，并由中心 InfiniBand 交换机来指挥流量。它的结构设计得非常紧密，大大提高了系统的性能、可靠性和有效性，能缓解各硬件设备之间的数据流量拥塞。而这是许多共享总线式技术没有解决好的问题，例如这是基于 PCI 的机器最头疼的问题，甚至最新的 PCI-X 也存在这个问题。因为在共享总线环境中，设备之间的连接都必须通过指定的端口建立单独的链路。

InfiniBand 的设计主要是围绕着点对点以及交换结构 I/O 技术，这样，从简单廉价的 I/O 设备到复杂的主机设备都能被堆叠的交换设备连接起来。InfiniBand 主要支持两种环境：模块对模块的计算机系统（支持 I/O 模块附加插槽）；在数据中心环境中的机箱对机箱的互连系统、外部存储系统和外部 LAN/WAN 访问设备。

InfiniBand 支持的带宽比现在主流的 I/O 载体（如 SCSI、Ethernet、Fibre Channel）还要高，另外，由于使用 IPv6 的报头，InfiniBand 还支持与传统 Internet/Intranet 设施的有效连接。用 InfiniBand 技术替代总线结构所带来的最重要的变化就是建立了一个灵活、高效的数据中心，省去了服务器复杂的 I/O 部分。

InfiniBand SAN 采用层次结构，将系统的构成与接入设备的功能定义分开，不同的主机可通过 HCA（Host Channel Adapter，主机适配器）、RAID 等网络存储设备利用 TCA（Target Channel Adapter，目标适配器）接入 InfiniBand SAN。

InfiniBand 应用于服务器群和存储区域网络（SAN），在这种环境中性能问题至关重要。该种结构可以基于信道的串口替代共用总线，从而使 I/O 子系统和 CPU/内存分离。所有系统和设备（一般称作节点）可通过信道适配器逻辑连接到该结构，它们可以是主机（服务器）适配器或目标适配器。该种结构（包括 InfiniBand 交换机和路由器）还可轻松实现扩展，从而满足不断增长的需求。InfiniBand 协议可满足各种不同的需求，包括组播、分区、IP 兼容性、流控制和速率控制等。

2）IB SAN 的特性

InfiniBand SAN 主要具有如下特性。

（1）可伸缩的 Switched Fabric 互连结构。

（2）由硬件实现的传输层互连高效、可靠。

（3）支持多个虚信道（virtual lanes）。

（4）硬件实现自动的路径变换（path migration）。

（5）高带宽，总带宽随 IB Switch 规模成倍增长。

（6）支持 SCSI 远程 DMA 协议（SRP）。

（7）具有较高的容错性和抗毁性，支持热插拔。

3）IB SAN 的应用与发展

在 InfiniBand 体系结构下，可以实现不同形式的存储系统，包括 SAN 和 NAS。基于 InfiniBand I/O 路径的 SAN 存储系统有两种实现途径：其一是 SAN 存储设备内部通过 InfiniBand I/O 路径进行数据通信，InfiniBand I/O 路径取代 PCI 或高速串行总线，但与服务器/主机系统的连接还是通过 FC I/O 路径；其二是 SAN 存储设备和主机系统利用 InfiniBand I/O 路径取代 FC I/O 路径，实现彻底的基于 InfiniBand I/O 路径的存储体系结构。

InfiniBand 有可能成为未来网络存储的发展趋势，原因如下。

（1）InfiniBand 体系结构经过特别设计，支持安全的信息传递模式、多并行通道、智能 I/O 控制器、高速交换机以及高可靠性、可用性和可维护性。

（2）InfiniBand 体系结构具有性能可伸缩性和较广泛的适用性。

（3）InfiniBand 由多家国际大公司共同发起，是一个影响广泛的业界活动。

InfiniBand 应用于服务器群和存储区网络，但它的模块化、可扩展的结构以及灵活性使其能够广泛应用于各种高性能 I/O 的结构。InfiniBand 将与其他标准兼容，如以太网和其他 LAN 及 WAN。InfiniBand 可作为一种“通用载体”技术进行应用，这使得它具备了解决大型集成问题的潜力。

3.2.8　备份系统及备份软件

1．数据备份结构

常见的数据备份系统主要有 Host-Base、LAN-Base 和基于 SAN 结构的 LAN-Free、Server-Free 等多种结构。

（1）Host-Based 备份方式。Host-Based 是传统的数据备份结构，该结构中磁带库直接接在服务器上，而且只为该服务器提供数据备份服务。一般情况下，这种备份大多是采用服务器上自带的磁带机，而备份操作通常是通过手工操作的方式进行的。另外，不同的操作系统平台使用的备份恢复程序一般也不相同，这使得备份工作和对资源的总体管理变得更加复杂。

Host-Based 备份结构的优点是数据传输速度快，备份管理简单；缺点是不利于备份系统的共享，不适合于现在大型的数据备份要求。

（2）LAN-Based 备份方式。LAN-Based 备份，在该系统中数据的传输是以网络为基础的。其中配置一台服务器作为备份服务器，由它负责整个系统的备份操作。磁带库则接在某台服务器上，在数据备份时备份对象把数据通过网络传输到磁带库中实现备份。

LAN-Based 备份结构的优点是节省投资、磁带库共享、集中备份管理；它的缺点是对网络传输压力大。

（3）LAN-Free 备份方式。LAN-Free 和 Server-Free 的备份系统建立在 SAN 的基础上。基于 SAN 的备份是一种彻底解决传统备份方式需要占用 LAN 带宽问题的解决方案。它采用一种全新的体系结构，将磁带库和磁盘阵列各自作为独立的光纤节点，多台主机共享磁带库备份时，数据流不再经过网络而直接从磁盘阵列传到磁带库内，是一种无须占用网络带宽（LAN-Free）的解决方案。

目前随着 SAN 技术的不断进步，LAN-Free 的结构已经相当成熟。LAN-Free 的优点是数据备份统一管理、备份速度快、网络传输压力小、磁带库资源共享；缺点是投资高。

（4）LAN Server-Free 备份方式。LAN Server-Free 备份方式是以全面的释放网络和服务器资源为目的的。它的核心是在 SAN 的交换层实现数据的复制工作，这样备份数据不仅无须经过网络，而且也不必经过应用服务器的总线，完全保证了网络和应用服务器的高效运行。目前一些厂商推出了自己在这方面的相关产品和解决方案，但是比较成熟且开放性好的产品还在进一步发展中。到目前为止，LAN Server-Free 技术已经成为所有相关厂商争相追逐的目标，无疑是备份技术领域内最大的热点，相信在不久之后，用户就可以真正享受到这一新技术带来的成果。

目前主流的备份软件，如 IBM Tivoli、Veritas 等，均支持上述 4 种备份方案。4 种方案中，LAN 备份数据量最小，对服务器资源占用最多，成本最低；LAN-Free 备份数据量大一些，对服务器资源占用小一些，成本高一些；LAN Server-Free 备份方案能够在短时间备份大量数据，对服务器资源占用最少，但成本最高。

2. 备份软件

一般磁带驱动器的厂商并不提供设备的驱动程序，对磁带驱动器的管理和控制工作完全是备份软件的任务。磁带的卷动、吞吐磁带等机械动作，都要靠备份软件的控制来完成。所以，备份软件和磁带机之间存在一个兼容性的问题，这两者之间必须互相支持，备份系统才能得以正常工作。

与磁带驱动器一样，磁带库的厂商也不提供任何驱动程序，机械动作的管理和控制全部由备份软件负责。与磁带驱动器相区别的是，磁带库具有更复杂的内部结构，备份软件的管理相应地也就更复杂。例如，机械手的动作和位置、磁带仓的槽位等。这些管理工作的复杂程度比单一磁带驱动器要高出很多，所以几乎所有的备份软件都是免费地支持单一磁带机的管理，而对磁带库的管理则要收取一定的费用。

（1）备份数据的管理。作为全自动的系统，备份软件必须对备份下来的数据进行统一管理和维护。在简单的情况下，备份软件只需要记住数据存放的位置就可以了，这一般是依靠建立一个索引来完成的。然而随着技术的进步，备份系统的数据保存方式也越来越复杂多变。例如，一些备份软件允许多个文件同时写入一盘磁带，这时备份数据的管理就不再像传统方式下那么简单了，往往需要建立多重索引才能定位数据。

（2）数据格式也是一个需要关心的问题。就像磁盘有不同的文件系统格式一样，磁带的组织也有不同的格式。一般备份软件会支持若干种磁带格式，以保证自己的开放性和兼容性，但是使用通用的磁带格式也会损失一部分性能。所以，大型备份软件一般还是偏爱某种特殊的格式。这些专用的格式一般都具有高容量、高备份性能的优势，但是需要注意的是，特殊格式对恢复工作来说是一个不小的隐患。

（3）备份策略制定是一个重要部分。需要备份的数据都存在一个 2/8 原则，即 20%的数据被更新的概率是 80%。这个原则说明，每次备份都完整地复制所有数据是一种非常不合理的做法。事实上，真实环境中的备份工作往往是基于一次完整备份之后的增量或差量备份。那么完整备份与增量备份和差量备份之间如何组合才能最有效地实现备份保护，这正是备份策略所关心的问题。

（4）工作过程控制。根据预先制定的规则和策略，备份工作何时启动，对哪些数据进行备份，以及工作过程中意外情况的处理，这些都是备份软件需要注意的问题。其中包括了与数据库应用的配合接口，也包括了一些备份软件自身的特殊功能。例如，很多情况下需要对打开的文件进行备份，这就需要备份软件在保证数据完整性的情况下，对打开的文件进行操作。另外，由于备份工作一般都是在无人看管的环境下进行，一旦出现意外，正常工作无法继续时，备份软件必须具有一定的意外处理能力。

（5）数据恢复工作。数据备份是为了恢复，所以这部分功能自然也是备份软件的重要部分。很多备份软件对数据恢复过程都给出了相当强大的技术支持和保证。一些中低端备份软件支持智能灾难恢复技术，即用户几乎无须干预数据恢复过程，只要利用备份数据介质，就可以迅速自动地恢复数据。而一些高端的备份软件在恢复时，支持多种恢复机制，用户可以灵活地选择恢复程度和恢复方式，极大地方便了用户。

3．备份介质

除了备份架构的新进展之外，在备份介质选择上，也出现了一些新的趋势。

传统上备份介质主要是以磁带设备为主，这主要是因为磁带在单位容量的成本上，较之其他介质具有非常大的优势。但是随着技术的发展进步，尤其是 ATA 技术的发展，硬盘的成本在迅速下降。现在，在一些场合下，磁盘作为备份介质其优势已经越来越明显。一些厂商正在着力劝说用户采用更加方便高效的磁盘代替磁带作为备份介质，更有一些厂商甚至推出了包含磁盘和备份软件的整体设备，即备份一体机。

事实上，磁盘作为备份介质的最大好处就是其介质管理工作的简化和性能的提升。前面提到过，一个磁带库的管理工作非常地复杂烦琐，如果考虑到对不同厂家的不同型

号的磁带库产品都提供良好支持，工作无疑是极其艰巨的。而磁盘介质则几乎不存在这样的问题。这也是备份软件厂商看好磁盘备份的理由之一。

然而，磁带介质本身的技术发展并没有受到这一理念的冲击。相反地，就在磁盘介质向离线存储领域进军的同时，磁带介质也借数据迁移技术的发展，大踏步地向在线存储领域发展着。

数据迁移技术也称为分层存储管理，是一种将离线存储与在线存储整合的技术。传统上，离线数据是静态的，无法实时地被访问，而数据迁移技术正是冲破这一限制，将离线数据与在线数据统一调度，从而实现所有数据的实时访问。与磁盘备份技术相反，这一技术的主要目的就是以一定的存储系统性能为代价，换取大型海量存储系统的总体拥有成本。如图 3-8 所示。

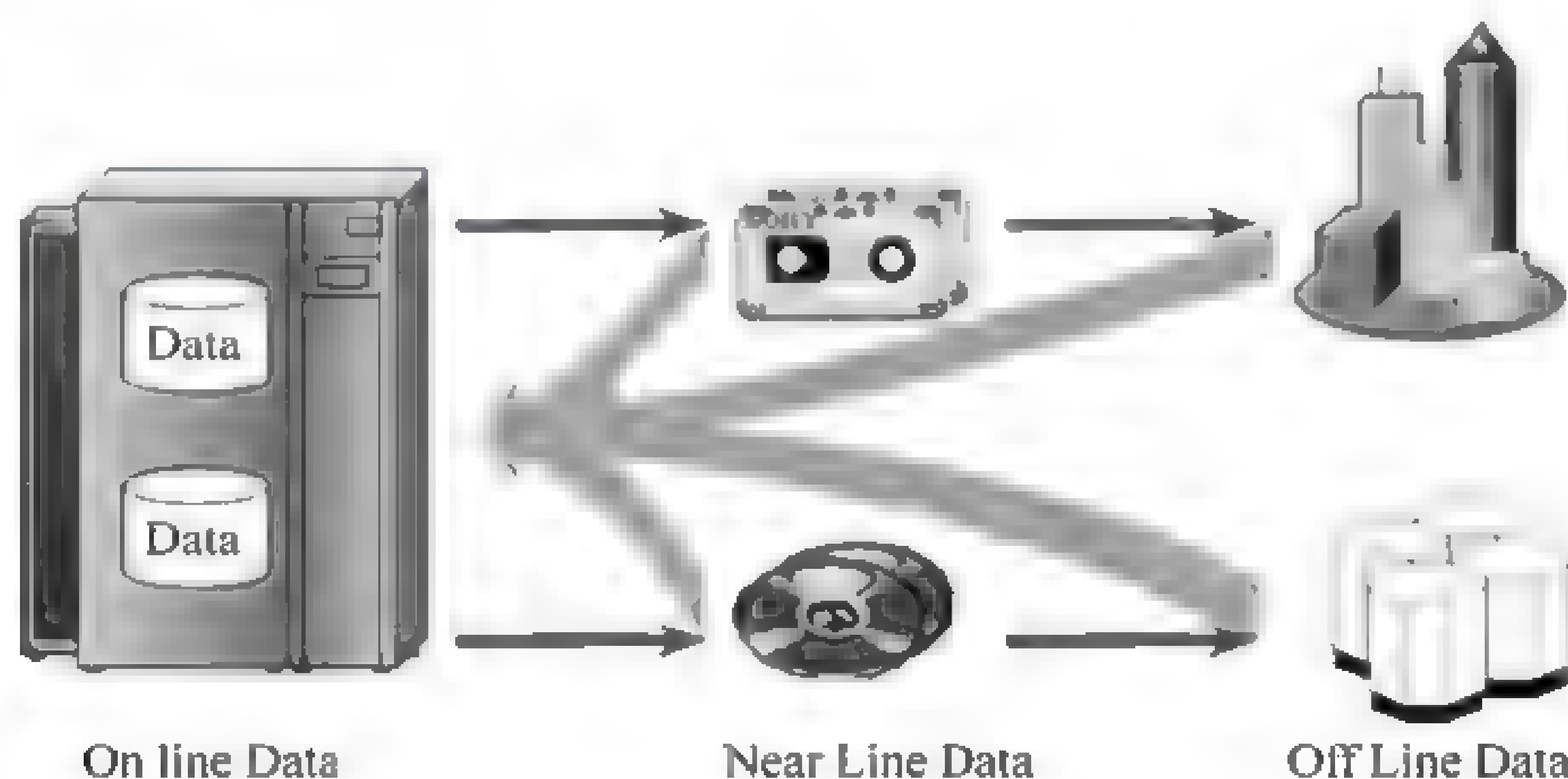


图 3-8　数据迁移的工作原理

数据迁移的工作原理比磁盘备份技术略为复杂。简单地说，就是将大量不经常访问的数据存放在磁带库等离线介质上，在磁盘阵列上只保存少量访问频率高的数据。当那些磁带介质上的数据被访问时，系统自动地把这些数据回迁到磁盘阵列中。同样，磁盘阵列中很久未访问的数据被自动迁移到磁带介质上。从某种意义上讲，磁盘阵列以一个磁带库的“中间缓存”的方式被使用，既保证了大多数情况下数据访问的响应性能，也避免了大量利用率低的数据长期占用成本较高的磁盘空间。

4．厂商及产品介绍

备份软件厂商中头把交椅当属 Veritas 公司。这家公司经过近几年的发展和并购，在备份软件市场已经占据了 4 成左右的份额。其备份产品主要是两个系列——高端的 NetBackup 和低端的 Backup Exec。其中，NetBackup 适用于中型和大型的存储系统，可以广泛地支持各种开放平台。NetBackup 还支持复杂的网络备份方式和 LAN-Free 的数据备份，其技术先进性是业界共同认可的。

Backup Exec 是原 Seagate Soft 公司的产品，在 Windows 平台具有相当的普及率和认可度，微软公司不仅在公司内部全面采用这款产品进行数据保护，还将其简化版打包在

Windows 操作系统中，我们现在在 Windows 系统中使用的“备份”功能，就是 OEM 自 Backup Exec 的简化版。2000 年年初，Veritas 收购了 Seagate Soft 之后，在原来的基础上对这个产品进一步丰富和加强，现在，这款产品在低端市场的占用率已经稳稳占据第一的位置。

Legato 公司是备份领域内仅次于 Veritas 公司的主要厂商。作为专业的备份软件厂商，Legato 公司拥有着比 Veritas 公司更久的历史，这使其具有了相当大的竞争优势，一些大型应用的产品中涉及备份的部分都会率先考虑与 Legato 的接口问题。而且，像 Oracle 等一些数据库应用干脆内置集成了 Legato 公司的备份引擎。这些因素使得 Legato 公司成为了高端备份软件领域中的一面旗帜。在高端市场这一领域，Legato 公司与 Veritas 公司一样具有极强的技术和市场实力，两家公司在高端市场的争夺一直难分伯仲。

Legato 公司的备份软件产品以 NetWorker 系列为主线，与 NetBackup 一样，NetWorker 也是适用于大型的复杂网络环境，具有各种先进的备份技术机制，广泛地支持各种开放系统平台。值得一提的是，NetWorker 中的 Cellestra 技术第一个在产品上实现了 Serverless Backup 的思想。仅就备份技术的先进性而言，Legato 公司是有实力挑战任何强大对手的。

除了 Veritas 和 Legato 这两大备份领域的巨头之外，IBM Tivoli 也是重要角色之一，其 Tivoli Storage Manager 产品是高端备份产品中的有力竞争者。与 Veritas 的 NetBackup 和 Legato 的 NetWorker 相比，Tivoli Storage Manager 更多地适用于 IBM 主机为主的系统平台，但其强大的网络备份功能绝对可以胜任任何大规模的海量存储系统的备份需要。

CA 公司是软件领域的一个巨无霸企业，虽然主要精力没有放在存储技术方面，但其原来的备份软件 ARCServe 仍然在低端市场具有相当广泛的影响力。近年来，随着存储市场的发展，CA 公司重新调整策略，并购了一些备份软件厂商，整合之后推出了新一代备份产品——BrightStor，这款产品的定位直指中高端市场。

3.3 其他资源设备

3.3.1 网络传真机

网络传真机（efax）也称电子传真机，是一种基于现有电话交换网（PSTN）和因特网的存储转发设备。它为现代办公提供了更高效、更经济、更环保的传真方式，是传统传真机的替代产品。

1. 网络传真机类别

目前网络传真机大致分为如下两类。

（1）软件网络传真机：通过在计算机上直接安装软件来实现传真功能。由于是单机模式，仅适用于个人或者小型企业。

（2）硬件网络传真机：在局域网内实现了用户对传真资源的共享，需一台硬件网络

传真设备，同时还需要一台传真服务器。这种方式加强了对传真的监控与统一的管理，适用于大中型企业和单位组织。

2．传真机选择标准

（1）稳定性。稳定的性能是选择传真服务系统的最基本指标。主要包括以下三条参考项。

① 看软件经过长时间运行后是否会出现僵死或瘫痪的现象。

② 看软件是否占用了过多的系统资源。

③ 看当传真量特别大时，服务器系统（包括软件部分和硬件部分）能否持续承受大任务量的压力而不出现异常。

（2）适用性。大多数的传真软件除基本的收发功能外，已经开发出许多辅助功能，如用邮件收发传真、传真审批、传真签章、传真编辑、短信通知、语音功能、与复合机的整合和集团免费传真等。但并不是所有的功能都是每个用户所必需的，而且各款软件对相同功能的实现都有其独特之处，需要根据实际需求和现有的工作环境选择适合的产品。

（3）兼容性。收发传真有多种设备、多种方式，就要求传真服务器对各式各样的传真方式给出的传真信号具有较强的兼容性。

（4）可扩展性。除了要考虑现有的传真线路、日均传真量、使用的人数和功能需求等外，还要考虑以后业务增长后的升级扩容问题。如果仅能满足目前需求，而不能满足日后的扩容需求，带来的不仅仅是重复投资，更重要的是传真数据无法延续、统一管理。

（5）易用性。要求软件操作时上手简单，易学，尽量方便和人性化。

（6）可集成性。许多单位和组织已经充分意识到信息化的必要性，随着各种信息化系统的引入，软件如 ERP、CRM 和 OA 等，硬件如高端复合机等，所要考虑的就不只是如何使用这些，更需要的是实现协同办公。为避免传真继续成为信息的孤岛，网络传真系统是否具有灵活的集成能力也是考量时不可忽视的一个方面。

3．典型实例

网络传真机连接电话交换网和网络传真服务器。网络传真服务器配备打印机、扫描仪，安装传真软件的服务器端，连接在局域网上。在需要收发传真的用户的计算机上安装网络传真软件的客户端，实现系统内各用户即时实现传真的收发，如图 3-9 所示。

系统实现的主要功能如下。

（1）每个用户都有属于自己的传真分机号，方便对外的联系。

（2）传统传真机与计算机用户实现互传。

（3）计算机用户像收发电子邮件一样收发传真。

（4）自动对所有接收和发送的传真进行电子存档，便于随时查看和分类整理。

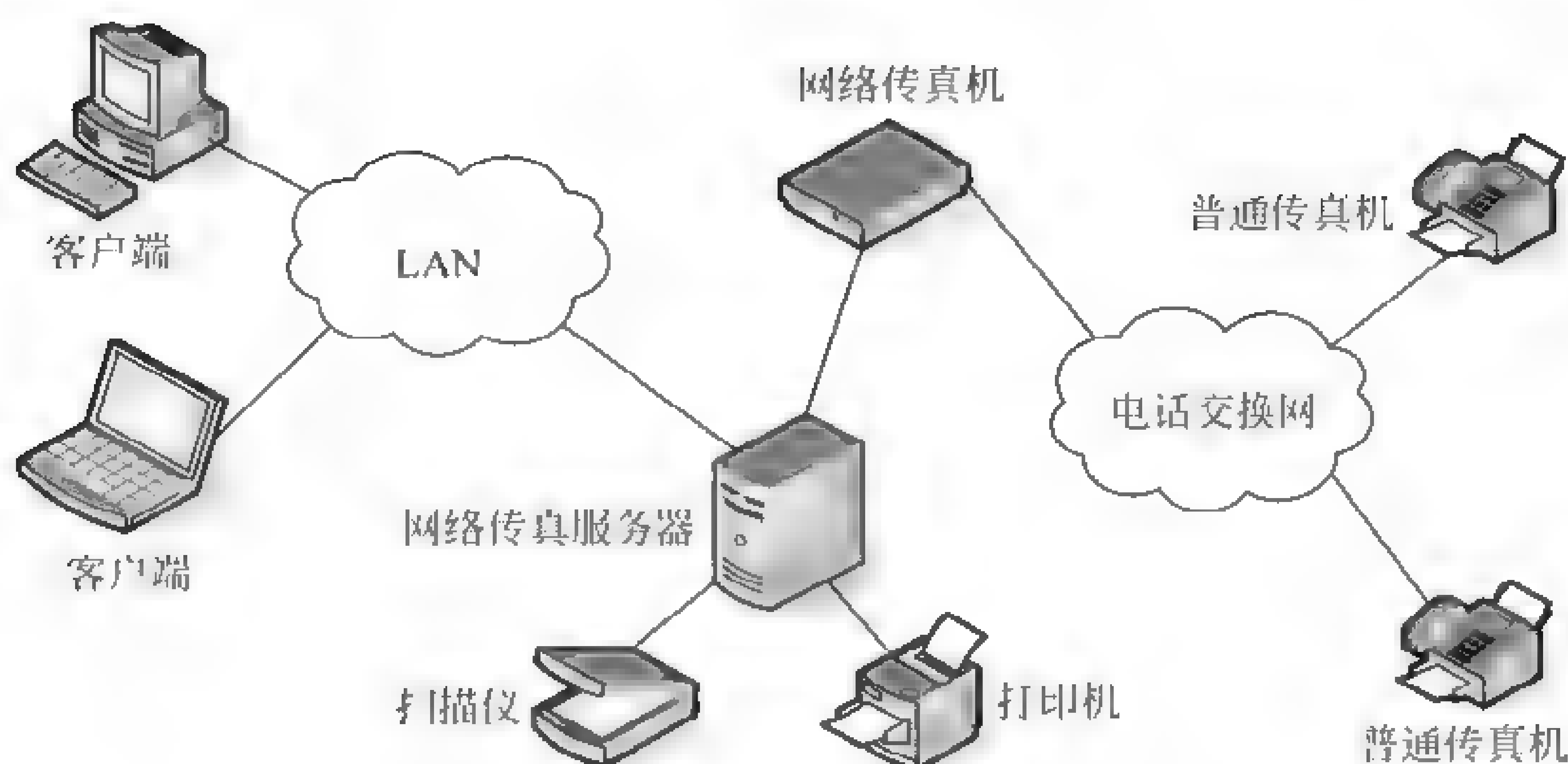


图 3-9　网络传真系统

（5）可以实现传真审批、传真签章和传真编辑等辅助功能。

3.3.2　网络打印机

网络打印机是指通过打印服务器将打印机接入局域网或者 Internet 的独立设备。网络打印机摆脱了一直以来作为计算机外设的附属地位，成为网络中一个独立的节点，一个信息管理与输出的终端，用户可以直接访问并使用网络打印机。

1．接入与控制

网络打印机要正常工作，一定要先接入网络。目前有两种接入的方式：一种是打印机自带打印服务器（也称内置打印服务器），打印服务器上有网络接口，只需插入网线分配 IP 地址便可工作；另一种是打印机使用外置的打印服务器，外置打印服务器一般配备一个外接电源，打印机通过并口或 USB 口与打印服务器连接，打印服务器再与网络连接。

网络打印机一般配有管理软件，通过管理软件可以从远程配置打印机的参数，查看并控制打印任务。网络打印管理软件需根据打印需求对网络连接性能进行优化，同时还需要与打印机内部控制器很好地匹配，具有一定的网络流量管理和打印队列管理能力。同时，用户可以通过它实现打印机的全方位管理和控制，同时还可以通过网络及时进行升级。

2．性能指标

网络打印机多为企业、单位办公所采用，应具有较高的打印速度和较好的打印效果。出于环保和打印成本的考虑，还应具有较低的打印噪声和较低的打印成本。网络打印机的传统打印部分大多采用激光打印方式，一些特殊情况则根据需要采用喷墨或其他打印方式。

网络打印机的硬件构成分为打印部分和网络部分，这两方面的性能共同决定了整机

的性能。综合考虑，有几个重要指标是值得关注的：打印质量、打印速度、处理介质能力、网络打印方式、设备接口、兼容性、管理软件和辅助功能。

（1）打印质量。打印质量是一个重要的指标，随着人们处理数据的类型越来越多，图像、图形、视频、动画、CAD、CAM 和 GIS 等高精度信息内容的打印也越来越多，网络打印质量的要求也越来越高。高端产品与低端产品的区别往往通过该指标来体现。不同的用户对打印质量有不同的需求，用户应根据自身需求来决定。

现在 600dpi 的分辨率已是激光打印机的最低标准，用户选购时应选择高于 600dpi 的机型。1200dpi 的机型是一般用户的较好选择。

（2）打印速度。网络打印机一般工作量比较大，打印速度直接影响办公效率。如果对打印速度要求较高，需选用打印引擎速度较快的机型。

此外，与普通打印机不同，网络打印机的打印速度还要受到内置处理器速度和内存大小的影响。网络打印机内置的处理器一般采用 RISC 处理器，工作频率从 50MHz 到 166MHz 或者更高。内存则是打印机专用的 DIMM 内存，一般具有升级功能，以便日后扩充内存。有的网络打印机还配有内置硬盘，打印时一次读取打印数据存储到硬盘上，不用再到服务器上重新读取，从而提高了批处理的速度。因此，是否选择内置的高主频的处理器，大容量内存或硬盘的网络打印机，用户应根据自身需求来决定。

（3）介质处理能力。介质处理能力也是衡量打印机性能的一个重要方面，首先就是打印机可打印的纸张幅面。常用的网络打印机的幅面有 A4 和 A3 两种，用户可以根据自己日常处理文档的幅面自行选择。一般 A3 幅面的机器价格要高出 A4 幅面的机器很多，在选购时应本着够用的原则；否则会造成资源的浪费。

网络打印机的打印任务较普通打印机更为繁重，因而它存储纸张的数量也是一个重要指标。网络打印机应有多种不同类型的存纸匣以满足不同需要，总容量大小至少超过千张。另外，彩色激光打印也日益普及，不过价格稍高。在这方面用户要根据自己的实际情况来选择。

（4）网络打印的方式。实现网络打印目前主要有两种：外置打印服务器+网络打印机，称为“外置式”；带内置打印服务器的网络打印机，称为“内置式”。两者的区别在于它们实现与网络相连的方式不同。外置式是通过外置打印服务器来转换从网线上传来的打印任务，然后通过打印机并口或 USB 口送到打印机上。而内置式是直接与网络相连，打印任务是直接从网络接收下来。外置式传输速率要受到并口或 USB 口速度的限制，内置式则直接利用打印机内部总线传输，速度比外置式快。外置式实现方法要容易些，可以充分利用已有的打印机资源，而内置式则只能用于专用型号的打印机。所以，低端的机型一般采用外置式的方案来实现网络打印，而高端的机型则采用内置网络打印服务器实现网络打印。

（5）设备接口。网络打印机内置打印服务器时，网络接口一般是自适应 10M/100M 的。可以直接连接到企业内部局域网上，并且支持 AppleTalk、IPX/SPX 和 TCP/IP 等网

络协议。兼容多种网络系统平台，包括 Windows、Macintosh 和 UNIX 等操作系统。

网络打印机采用外置打印服务器时，则应注意在接口上要与公司实际网络接口类型保持一致，否则所购买的打印服务器乃至打印机都不能在自己的网络上使用。一般在打印服务器上都会有多种连接接口供选择，如 RJ-45 的“以太网接口”和“令牌网”接口、BNC 的同轴电缆接口、九针串行通信接口及 Mini-Din 8 八芯接口等。选择时一定要注意打印服务器所适应的接口类型。

（6）兼容性。目前网络打印机的主要生产厂家，在打印服务器标准上并没有达成一致，也就是说彼此还不能互相兼容，且多数生产厂家把打印服务器内置在打印机主板上，但也有少许型号的网络打印机的打印服务器是可选配的，所以这时首先就要看清楚你所选购的打印服务器是用在什么型号的网络打印机上。

（7）管理软件。网络打印机与其他普通打印机的一个主要区别就在于不仅需要打印机的驱动程序，而且还需要一个网络打印机管理软件来管理网络打印机。随着网络技术的飞速发展，网络打印机的管理软件在管理方式上也得到了质的飞跃，一些专业的打印机制造商，如 HP 公司等就把网络打印机的管理软件从本地计算机搬到了 Web 上了。如果有这方面的要求，那就要选择能应用此类管理软件的网络打印机。

（8）辅助功能。在其他的一些辅助功能上，各厂商也大都有各自的特色，如 EPSON 的“作业平衡”、HP 的 ColorSmart II 等，在选择时应该多了解所选择的网络打印机的此类辅助功能。

3.3.3　网络视频会议系统

视频会议系统是一种支持远距离通信，使处于不同地域的人进行实时信息交流、开展协同工作的应用系统。该系统不仅能实时传输视频和音频信息，使各成员可以远距离进行直观、真实的视音频交流，还可利用其他媒体技术的支持，帮助各成员处理会议中的共享信息。作为一种现代通信方式，视频会议也是一个国家或地区通信发展水平的重要标志之一。

1．系统工作原理

目前在网络上运行的视频会议按技术不同可分为两类：一是基于单播网络和 H.323 协议族的视频会议；二是基于组播网络和开放软件的视频会议。

基于单播网络和 H.323 协议族的视频会议系统，通过多点控制单元（MCU）建立视频会议网络的控制平台，实现视频会议终端任意多点的视频会议功能。从理论上说，只要 IP 网络铺设到的地方均可以安装视频会议终端，成为会议室或远程会议点。多点视频会议的实施还需要做很多工作，如通过 BGP 调整配置来保证视音频数据传输流畅，使用基于 LDAP 协议的分布式目录服务完成动态地址之间的通信等，以保证高质量视频会议的完成。

基于 IP 组播网络的视频会议系统利用 IP 组播（Multicast）技术可构建具有组播能

力的网络。组播允许路由器一次将数据包复制到多个通道上，降低了网络带宽要求，有效节省传输带宽，这对于需要在多点之间传输流媒体的视频会议尤其具有重要意义。同时，IP 组播视频会议系统平台不需要 MCU，通过软件来实现视频会议终端任意多点的视频会议功能，大大节省了系统成本。

典型的 H.323 协议体系涉及终端设备、视频、音频和数据传输、通信控制、网络接口方面的内容，还包括了组成多点会议的多点控制单元、网关（GW）以及网守（GK）等设备。

视频终端包括可软件升级的 H.323 编码器、摄像机、话筒和屏幕等。

网关的主要功能是信令处理 H.323 协议功能、语音编码和解码以及路由协议处理等功能，对外分别提供与 PSTN 连接的中继接口以及和 IP 网络连接的接口。

网守的主要功能是地址解析、带宽管理、用户认证、路由管理、安全管理和区域管理。

多点控制单元用于支持三个以上端点设备的会议。在 H.323 系统中，一个多点控制单元由一个多点控制器（MC）和几个多点处理器（MP）组成，可以不包含 MP。

2. 解决方案

现阶段视频会议系统解决方案主要有硬件和软件两类，两者各有其特点。一般而言，硬件视频系统图像质量高，价格比软件视频系统高出许多倍，对各个节点也有硬件环境要求。

1）基于硬件的视频会议系统

随着网络技术的不断发展，视频会议网络端设备技术也不断发展，传统的语音采用 PSTN 传输、视频采用 ISDN(H.320)的传输方式最终被 IP（H.323）网络传输所代替。基于 IP 技术的视频会议系统为用户提供语音、视频和数据的三网合一的服务。硬件会议系统的主要技术特点如下。

（1）符合国家规定的行业技术标准，如 ITU-T 的 H.323、H.320 标准。

（2）音频支持 G.711、G.722 和 G.728 等协议。

（3）视频支持 H.261、H.263、H.263+和 H.264 等协议。

（4）采用 MCU 控制管理，MCU 具有可扩展性。

（5）具有双视、双流等新功能。

硬件视频会议系统由于采用的是硬件编解码技术，要求的网络带宽在 384K 以上，具有良好的显示效果，因此，显示终端多采用大屏幕电视机和投影机。

2）基于软件的视频会议系统

软件视频会议可以利用现有的 Internet 环境和计算机设备，能够提供较高的音视频质量和更为丰富的数据协作功能。软件会议系统主要的技术特点如下。

（1）兼容 ITU-T 的 H.323、H.320 标准。

（2）视频支持 MPEG4、H.264 等视频压缩算法。

（3）音频采用 G.723.1、G.711 和 GIPS 压缩算法。

（4）采用服务器作为 MCU，通用性好。

软件的视频会议系统着力于解决低带宽下的网络视频会议的需要，主动降低了图像的传送帧数和分辨率（对应关系如表 3-8 所示），因此显示终端常采用计算机显示屏，在网络带宽较高且比较稳定的情况下，也可采用大屏幕电视或投影机。

表 3-8　带宽、帧数和分辨率对应关系表

带　　宽	图像分辨率	传输速率（帧/秒）
384K 以上	640×480	15～30
	CIF（352×288）	30
128～384K	CIF（352×288）	15～25
	QCIF（176×144）	20～25
64～128K	QCIF（176×144）	15～20
56K	QCIF（176×144）	4～6

3. 网络视频会议系统选型

1）制定具体需求

（1）要考虑是上软件视频还是硬件视频会议系统，还是软件硬件相结合。

（2）要考虑是需要国外知名品牌产品，还是国内知名产品，还是基本实现视频功能。

（3）确定视频会议同时在线的点数（尤其是对软件视频会议，因为很多点都可以装客户端的），硬件则以建设的会议室数或办公室数来确定。

（4）确定视频会议网络情况，主要是内部局域网还是专线网，还是因特网。

（5）确定会议带宽（一般是 384K、768K、1M、1.5M、2M、4M、8M 等，以 768K、1M、1.5M、2M 为多）。

（6）确定是否需要高清视频。

（7）判断是否需要双流，主要是计算机资料或第二路视频显示使用，多用在数据会议和远程培训上。

（8）判断是否需要远控（主要是远程控制摄像机）。

（9）如果是硬件视频会议终端，判断是需要机顶盒式产品还是分体式产品。

（10）注意不同品牌的视频会议终端摄像机的配置情况，是内置还是外购。

（11）是否需要会议录制、点播或直播功能。

（12）如果是硬件视频会议，判断是否需要电视墙功能（就是将从 MCU 取得的信号分路独立显示在不同的监视设备上）。

2）设备选型原则

（1）关键设备选用基于 IP 的网络视频会议产品，符合当前视频会议系统发展方向。

（2）系统具备多媒体通信应用平台的特性，可扩展性强，能满足未来发展要求。

（3）视频方面支持 MPEG-4 压缩技术，支持多种视频格式，支持多分屏显示及任意切换。若需高清视频，则系统需支持 H.264 视频标准。

（4）音频方面语音清晰流畅，支持音频双向传输。

（5）具备必要的辅助功能，如电子白板、远程 PPT 等。

（6）界面友好、使用方便、操作简捷。

4. 系统部署实例

网络视频会议系统部署实例如图 3-10 所示。

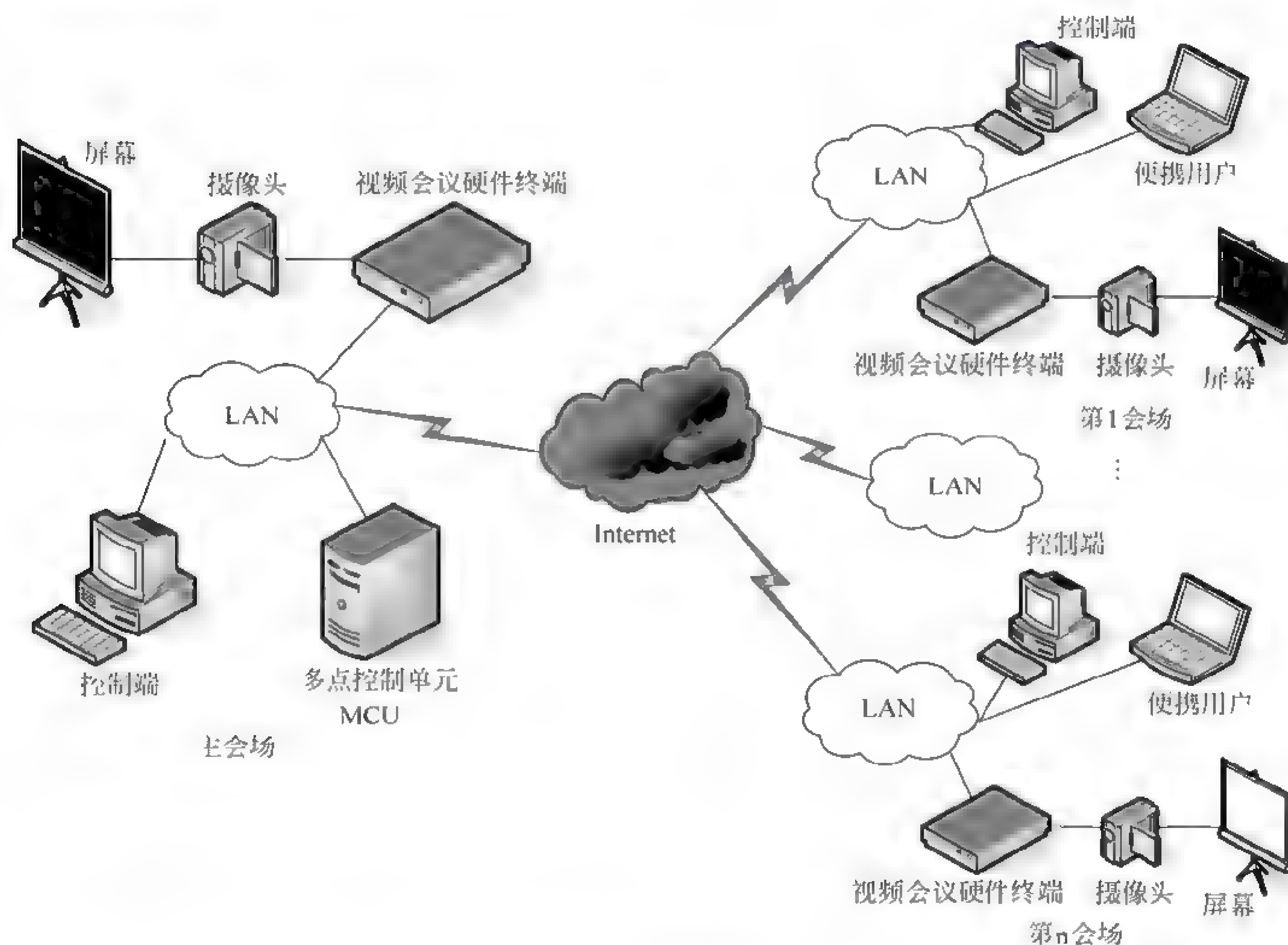


图 3-10 网络视频会议系统

1）设备配置

由两部分组成，即主会场的设备和分会场的设备。主会场的设备包括服务器（多点控制单元）、屏幕、视频会议硬件终端、摄像头（或摄像机）、麦克风和音箱；分会场的设备包括视频会议硬件终端、屏幕、高速球机、麦克风和音箱。

2）系统结构组成

（1）主会场：核心设备视频服务器、视频会议硬件终端。视频信号和音频信号通过

视频会议硬件终端传输到网络中。系统服务器端软件安装在主会场，并在主会场控制端计算机里安装客户端软件，管理员可通过视频软件随意跟任何一个分会场的参会人员通话，并且可以通过监控软件对分会场的图像和声音进行控制。

（2）分会场：核心设备是视频会议硬件终端，视频信号和音频信号直接通过视频会议硬件终端与网络连接。视频会议硬件终端与分会场的屏幕相连，分会场的与会人员可以通过麦克风与主会场的人员通话，主会场的图像和声音可以通过电视和音箱来接收。

3.3.4　网络电话系统

网络电话系统是一种利用 VoIP（Voice over Internet Protocol）技术，透过因特网实时传输音频信息及实现双边对话的网络应用系统。网络电话系统一般包括语音网关、网守、网络电话机等设备。

语音网关扮演公众电话网络与 IP 网络间的桥梁角色，负责不同网络之间信令和控制信息的转换以及媒体信息变换和复用。它的主要功能有语音的压缩/解压缩、封包化、封包遗失补正、回音的消除、计费和与网络流量的监控等。有时也含有网关管理的功能，如安全查验、用户授权、保存通话记录资料、频宽的动态管理、实时性的网络资源管理和平衡流量等。网守处于高层，提供对端点（终端、网关、多点控制单元统称为端点）和呼叫的管理功能，是网络电话系统中的重要管理实体。网守有地址解析、接入控制、带宽管理和区域管理这 4 项基本功能。此外，还能提供呼叫控制信令、呼叫管理等其他功能。网络电话机是在 IP 网络上遵循一定的协议标准进行实时通信的端点设备。

1．方案及设备选型

对于网络电话的部署，有不同的通信方案，根据具体需求在不同情况下又需要采取不同的组网方案和设备。目前网络电话系统涉及的产品包括 IP 网关、IP PBX（IP 电话交换机）和 PC PBX（基于 PC 服务器的小型 IP 电话交换机）。

1）方案一　VoIP 网关+网守+PBX+ IP 电话/模拟电话

VoIP 网关提供传统的语音接口，与企业现有的电话交换机（PBX）或集团电话连接，同时连接 IP 网络，完成模拟语音信号与 IP 数据信号之间的相互转换。其主要特点是充分利用现有的网络资源，节省用户的长途话费，与现有的传统电话交换机或集团电话相结合，可以将传统语音电话转移到 IP 电话上。VoIP 网关产品作为一种成熟的 IP 电话解决方案，在许多大型单位中也得到应用。同时，一些小型 VoIP 网关产品的出现，也会给中小型用户带来极大好处。这类产品一般能够提供 1 路、4 路或 8 路电话中继接口，同时提供简单的路由功能和网络接口，能够方便地将单位分支机构的电话交换机或集团电话通过 IP 网络连接起来。

VoIP 网关型的应用是将 IP 语音网关的专用接口同总部或分支机构的 PBX 直接相连，当需要打长途电话时，将话音转到 VoIP 网关上，通过因特网传输。用户在使用时只需在分机上先拨 IP 电话特服号，便可直接拨打 IP 电话。

在这个方案中，若要像普通电话那样数字号码拨号，就得经过网守的路由管理，这种设备较昂贵，小型单位可借用电信运营公司的网守来实现，否则只能拨打 IP 号。网守处于高层，提供对端点的呼叫管理功能。

2）方案二　IP PBX+PBX+ IP 电话/模拟电话

IP PBX 是一种基于 IP 的电话交换系统，具有传统 PBX 交换机的所有功能，它的目标是取代单位内部原有的 PBX。这个系统可以完全将话音通信集成到 IP 网络中，从而建立能够连接分布各地办公地点和员工的统一语音数据网络。IP PBX 最显著的特征是一个集成通信系统，通过因特网，仅需要单一设备即可为用户提供语音、传真、数据和视频等多种通信方式，建立中、小型的呼叫中心。在采用 IP-PBX 构建的 VoIP 平台上，用户具有可移动的特性，形象地说，就是同一个用户在 A 地用的是 011 的号码，到了 B 地还是 011 的号码，号码随着人走。IP-PBX 还支持语音信箱、多方会议和视频会议等传统 PBX 没有的功能，有助于移动办公和异地协同办公。

在总部和分支机构均部署 IP PBX，内部人员可以使用 IP 电话或是普通模拟电话连接到不同的 IP PBX 上。对于经常出差的人士，可以使用 SIP 的软件电话，通过笔记本计算机实现移动通话。

若总部和所有分支单位都是使用固定公网 IP 上因特网，各点的 IP PBX 就可以通过 IP 对 IP 实现"点对点"通信，能直接找到双方。若使用的是浮动 IP，IP 不断变化就需要通过网守来进行地址解析了，浮动 IP 节点会在 IP 变更时向 GateKeeper 进行 IP 更新的通知动作。若 IP PBX 集成有网守或可添加网守模块，那网守可由总部设定；若没有，则需要通过注册 GateKeeper 虚拟运营商来解决。

3）方案三　PC PBX+PBX+ IP 电话/模拟电话

基于 IP PBX 交换机的平台虽然较稳定，但价格昂贵，规模较小的单位可能无法接受。虽然这些单位自身的规模较小，但同样也需要稳定、性能好的系统的保证。于是，PC PBX 应运而生，业界通常称为"应用服务器"。这类系统基于 PC 服务器单独用电话板卡加软件实现了 PBX、自动电话应答（IVR）和自动呼叫分配（ACD）等功能。

PC PBX 综合了 VoIP 网关和 IP PBX 的特点，可以使用现有电话线路和电话机，使用 VoIP 板卡实现跨 IP 网络的长途电话。PC PBX 产品提供了灵活拓展的余地，使得用户能得到功能丰富的 IP 通信，且无须高昂的费用成本。

构建基于 PC 服务器+呼叫管理软件的 PC PBX 系统作为在总部设立内部 IP 电话网的控制中心（PC PBX）。该控制中心以软件方式工作，安装在一台服务器内，采用数字中继网关与原有 PBX 的 E1 中继接口相连。在控制中心的服务器上对 IP 电话号码进行分配，或对原分机电话的拨号方式进行设定。在各分支机构安装 IP 话机或语音网关，根据实际需求为 IP 话机、语音网关配置公网电话号码。

该方案除安装和配置都非常简便外，还具有良好的可扩展性，在带宽许可的范围内，直接加装语音网关并分配号码，便可立刻实现电话扩容。在保持原 PBX 编号方案不变的情况下，系统内通话只需拨分机号。

2．系统部署实例

关键设备：在总部部署网关和网守设备各一台，各分部部署一台网关。语音网关提供了 E1 中继接口和模拟接口，同时提供简单的路由功能和网络接口，方便地将各分部的电话通过 IP 网络连接起来。网守负责实现地址解析、接入控制、带宽管理和区域管理等核心控制功能，如图 3-11 所示。

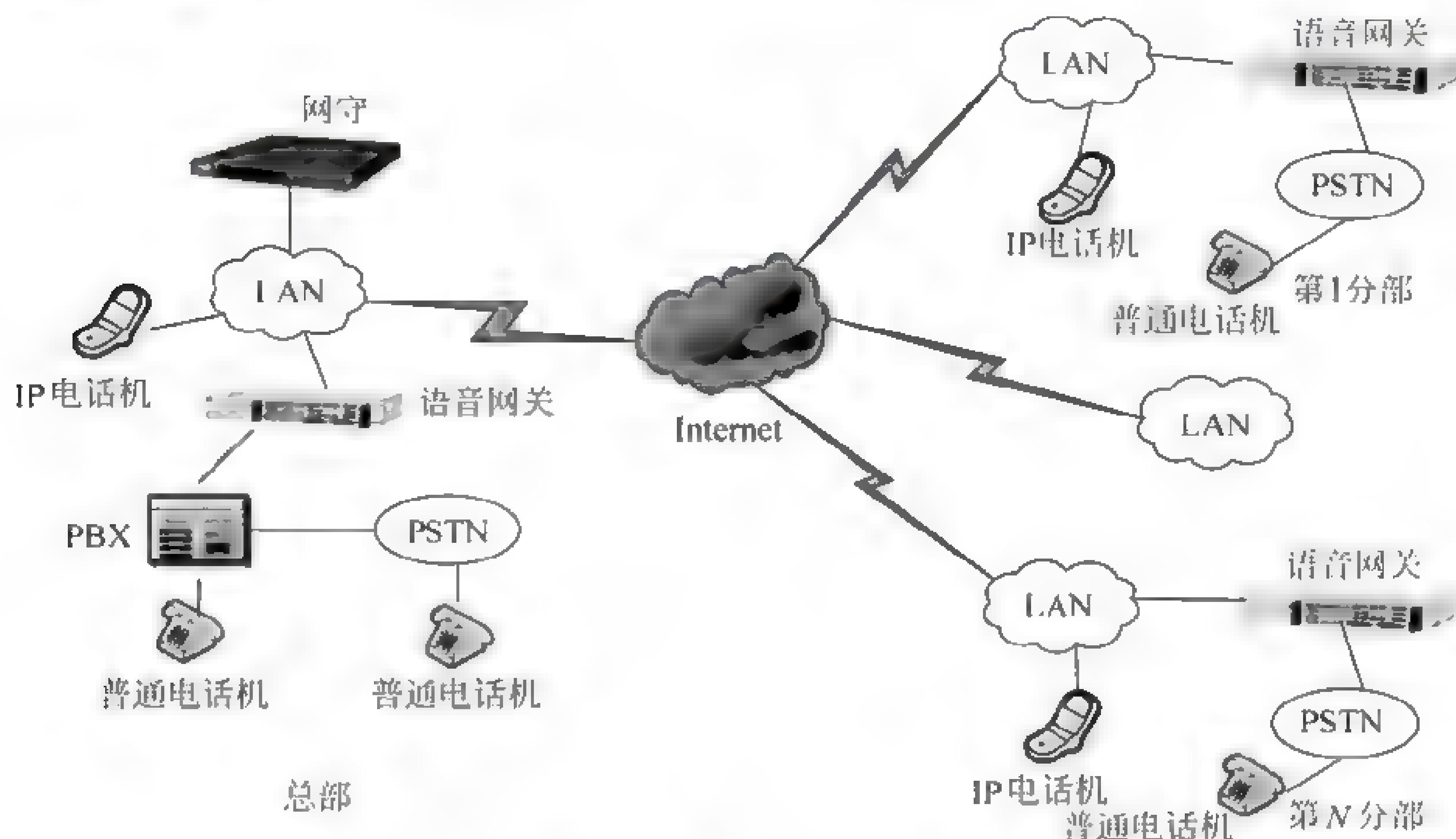


图 3-11　网络电话结构图

功能：实现 N 个分部 VoIP 通话，各分部内部也能实现各自的 VoIP 通话。

号码规划：一般有两种号码规划方法，一种是纯的 VoIP 电话方案，自定义本单位内部的 VoIP 电话号码；另一种是使用原有的电信市话号码作为 VoIP 电话的电话号码，并做“1∶1 绑定”。

（1）自定义 VoIP 电话号码方案。这种方案一般使用三位或四位数字来规划，号码随意制定。这种 “纯” 的 VoIP 电话组网，也就是没有接入市话线路，因此不需跟市话号码做“1∶1 绑定”。采用自定义三位（数字）小号，在前面加各市区号来组合成 VoIP 电话号码，本地（指语音网关内部）通话直拨小号，跨市局通话，前面加拨区号，由网守来路由。

（2）使用原有电信市话号码作为对应的 VoIP 电话号码。这种方案使用桌面电话的原有电信市话号码作为内部 VoIP 电话的号码，这样最终使用电话的用户还是按照原来拨号方式打电话，用户并不知在打的电话是经过 IP 网络还是经过电信公司的市话线路。在 VoIP 网络通畅时，电话是优先经过 VoIP 链路通话的，只有在 VoIP 出现故障或打外线电话时，才会通过电信公司市话线路通话。

第4章　网 络 安 全

4.1　恶意代码

4.1.1　恶意代码的定义与分类

1．恶意代码的定义

未经用户授权便干扰或破坏计算机系统/网络的程序或代码被称之为恶意软件（malware）或恶意代码。malware 这个单词来自于 malicious 和 software 两个单词的合成，是恶意软件的专业术语，专指那些泛滥于网络中的恶意代码。

恶意代码具有如下共同特征。

（1）具有恶意的目的。

（2）自身是计算程序。

（3）通过执行发生作用。

2．恶意代码分类

恶意代码包含的种类很多，主要类型有计算机病毒、网络蠕虫、特洛伊木马、后门、DDoS 程序、僵尸程序、Rootkit、黑客攻击工具、间谍软件、广告软件、垃圾邮件和弹出窗体程序等。

（1）计算机病毒。计算机病毒（computer virus）最早是由美国计算机病毒研究专家 F.Cohen 博士提出的。计算机病毒的定义有多种，较为通用的定义为：计算机病毒是一段附着在其他程序上的、可以自我繁殖的程序代码。复制后生成的新病毒同样具有感染其他程序的功能。

1994 年 2 月 18 日，我国正式颁布实施了《中华人民共和国计算机信息系统安全保护条例》，在《条例》第二十八条中明确指出："计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码"。此定义具有法律性、权威性。

随着网络的快速发展，计算机病毒的传播行为和感染方式也开始逐渐发生改变，笔者对计算机病毒定义如下。

计算机病毒是一段可以通过自我传播的破坏性程序或代码，其需要用户的干预来触发执行，通常其使用系统的正常功能进行传播。

（2）网络蠕虫。网络蠕虫是一段可以通过网络进行自我传播的破坏性程序或代码，其不需要用户的干预来触发执行。其通常利用系统漏洞进行传播，因而其可以直接获得

对方系统的控制权而自动执行蠕虫代码或程序。

（3）特洛伊木马。特洛伊木马是一个程序，它看起来具有某个有用的或善意的目的，但是实际上掩盖着一些隐藏的恶意功能。其欺骗用户或者系统管理员安装，或者在计算机上与“正常”的程序一起混合运行，将自己伪装得看起来属于该系统。

特洛伊木马通常由被控制端和控制端组成，其对用户的个人隐私和机密数据造成极大威胁。

（4）后门。后门是一个允许攻击者绕过系统中常规安全控制机制的程序，它按照攻击者自己的意图提供通道。后门的重点在于为攻击者提供进入目标计算机的通道。

（5）DDoS 程序。分布式拒绝服务（Distributed Denial of Service，DDoS）攻击是指借助于客户端/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DoS 攻击，从而成倍地提高拒绝服务攻击的威力。它是一种分布、协作的大规模攻击方式，主要瞄准比较大的站点，像商业公司、搜索引擎和政府部门的站点。图 4-1 描述了传统的 DDoS 模型。

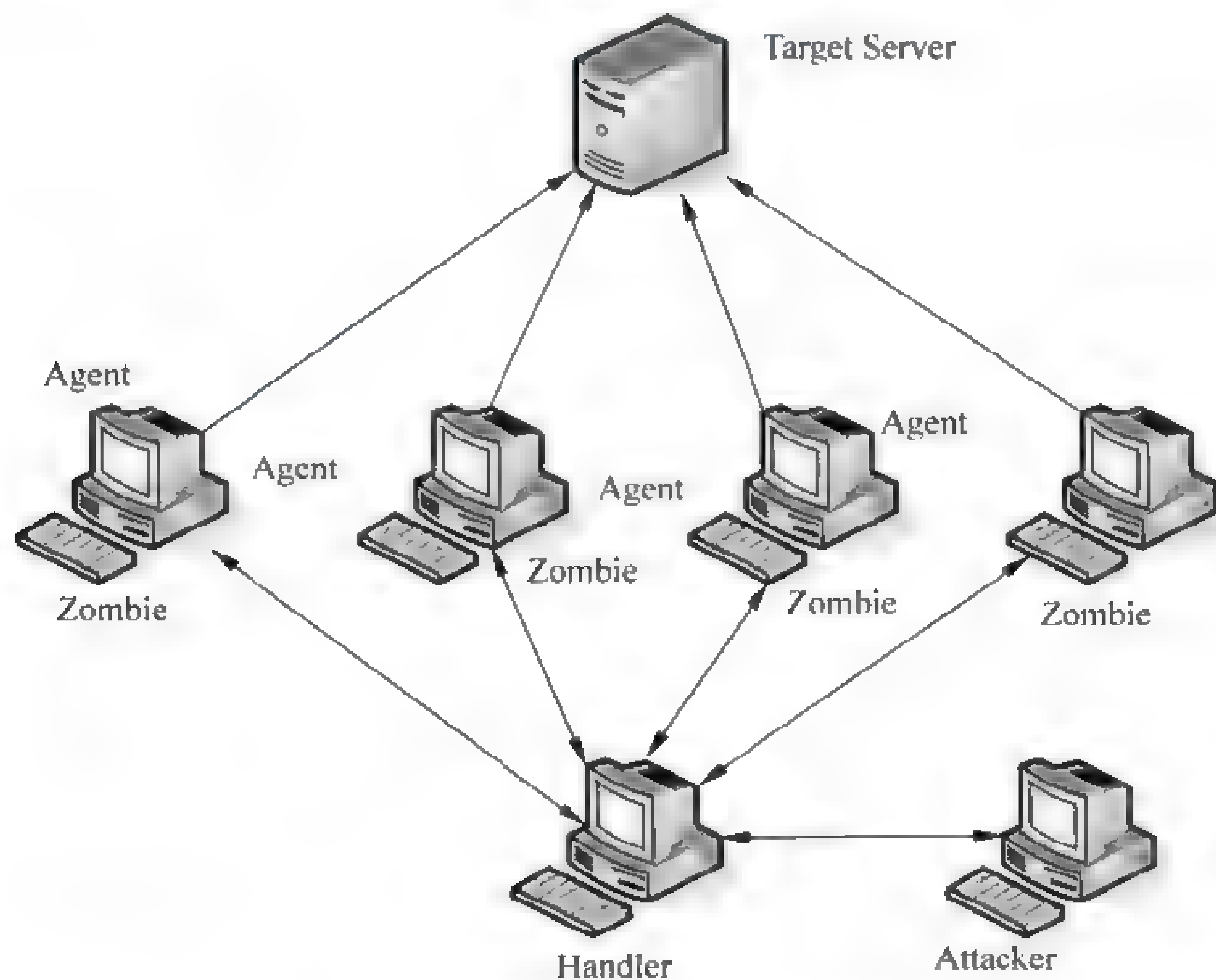


图 4-1　传统的 DDoS 模型

（6）僵尸程序（bot）。僵尸程序是秘密运行在被控制计算机中、可以接受指定命令和执行指定功能的程序。僵尸程序和命令控制服务器、控制者一起组成的可通信、可控制的网络被称为僵尸网络（Botnet）。控制者可以通过命令控制服务器对僵尸网络中的僵

尸计算机发送命令、进行控制，图 4-2 描述了 Botnet 的基本网络结构。根据命令控制所使用的协议的不同，僵尸网络又可分为 IRC Bot、AOL Bot 和 P2P Bot 等。其中，IRC Bot 最为常见。

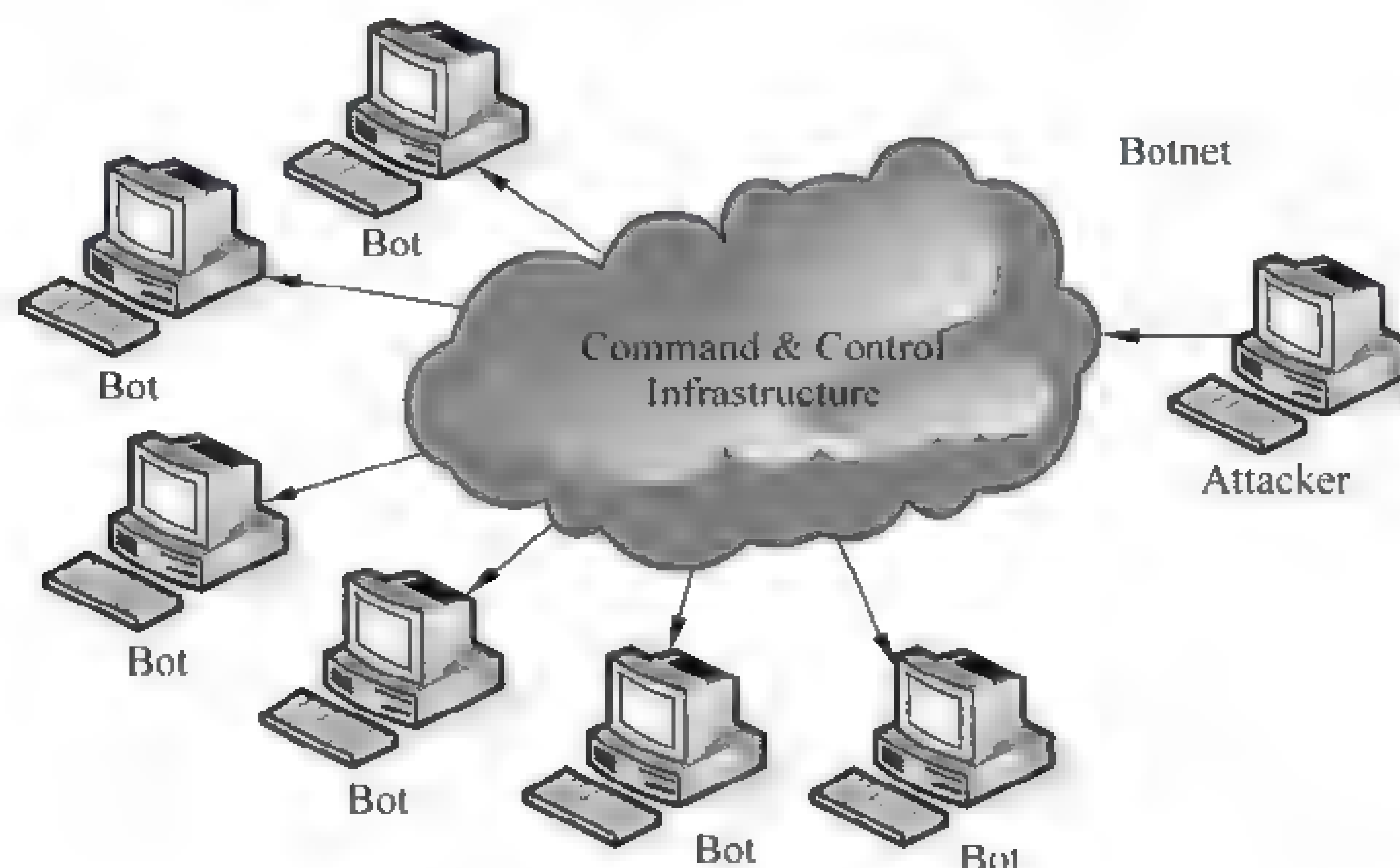


图 4-2　Botnet 的基本网络结构

僵尸网络与其他攻击方式最大的区别在于攻击者和僵尸主机之间存在着一对多的控制关系，而正是这种一对多的控制关系，使得攻击者能够以极低的代价高效地控制大量的资源并为其服务，这也是僵尸网络攻击模式近年来受到黑客青睐的根本原因。

（7）Rootkit。Rootkit 通过修改现有的操作系统软件，使攻击者获得访问权并隐藏在计算机中。

（8）黑客攻击工具。黑客攻击工具是指可以用来协助攻击者入侵计算机系统的一系列工具的集合。包括各种扫描器、Exploit 和密码嗅探工具。

（9）间谍软件。间谍软件是一种能够在用户不知情的情况下，在其计算机上安装后门、收集用户信息的软件。用户的隐私数据和重要信息会被“后门程序”捕获，并被发送给黑客、商业公司等。这些“后门程序”甚至能使用户的计算机被远程操纵，组成庞大的“僵尸网络”，这是目前网络安全的重要隐患之一。

（10）广告软件。广告软件是指未经用户允许，下载并安装或与其他软件捆绑通过弹出式广告或以其他形式进行商业广告宣传的程序。安装广告软件之后，往往造成系统运行缓慢或系统异常。此类软件往往会强制安装并无法卸载；在后台收集用户信息牟利，危及用户隐私；频繁弹出广告，消耗系统资源，使其运行变慢等。

（11）垃圾邮件（spam）。一般来说，凡是未经用户许可就强行发送到用户邮箱中的任何电子邮件都是垃圾邮件。垃圾邮件可以分为良性的和恶性的。良性垃圾邮件是各种

宣传广告等对收件人影响不大的信息邮件；恶性垃圾邮件是指具有破坏性的电子邮件。垃圾邮件占用大量的网络带宽，造成邮件服务器拥塞；侵犯收件人的隐私权，欺诈收件人；严重影响 ISP 服务形象；还常常被黑客利用，对 PC 造成严重破坏。

（12）弹出窗体（popups）。弹出窗体通常存在于广告或其他商业服务，它出人意料地弹出到你的屏幕上。跟垃圾邮件一样烦人，且有些具有破坏性。

在对恶意代码的分类上，特别是在对病毒和蠕虫的区分上，存在各种不同的理解。例如，反病毒公司通常将所有的恶意代码都归于病毒集合之中。如有些反病毒公司对蠕虫定义是以“网络复制过程是否主动”为依据来区分网络蠕虫与传统病毒。而本文中是以其是否需要人为干预来触发执行，是否使用了系统漏洞为判断依据。

4.1.2　常见的恶意代码命名规则

反病毒公司为了方便管理，会按照恶意代码的特性，将恶意代码进行分类命名。虽然每个反病毒公司的命名规则都不太一样，但大体都是采用一个统一的命名方法来命名的。目前绝大多数反病毒公司将所有的恶意代码都纳入在计算机病毒范畴内，因此在本节出现的病毒是指广义上的计算机病毒，即恶意代码。

恶意代码的一般命名格式为：

```
<恶意代码前缀>.<恶意代码名称>.<恶意代码后缀>
```

恶意代码前缀是指一个恶意代码的种类，它是用来区别恶意代码的种族分类的。不同种类的恶意代码，其前缀也是不同的。例如，常见的木马程序的前缀是 Trojan、网络蠕虫的前缀是 Worm 等。前缀表示了该病毒发作的操作平台或者病毒的类型，如 Macro、PE、Win32、Win95、VBS、BackDoor、Trojan 和 Worm 等。

如果没有前缀，一般表示 DOS 操作系统下的病毒。

恶意代码名称是指一个恶意代码的家族特征，是用来区别和标识恶意代码家族的，如著名的 CIH 病毒的家族名都是统一的 CIH、振荡波蠕虫的家族名是 Sasser。

恶意代码后缀是指一个恶意代码的变种特征，是用来区别具体某个家族恶意代码的某个变种的。一般都采用英文中的 26 个字母来表示，如 Worm.Sasser.b 就是指振荡波蠕虫的变种 B，因此一般称为“振荡波 B 变种”或者“振荡波变种 B”。如果该恶意代码变种非常多（也表明该病毒生命力顽强），可以采用数字与字母混合表示变种标识。

综上所述，一个恶意代码的前缀对于快速地判断该程序属于哪种类型的恶意代码是有非常大的帮助的。通过判断恶意代码的类型，就可以对这个恶意代码有个大概的评估（当然，这需要积累一些常见恶意代码类型的相关知识）。而通过恶意代码名可以利用查找资料等方式进一步了解该恶意代码的详细特征。恶意代码后缀能让用户或者反病毒工作者知道恶意代码是哪个变种。

下面附带一些常见的恶意代码前缀的解释（针对用得最多的 Windows 操作系统）。

（1）系统病毒。系统病毒的前缀为 Win32、PE、Win95、W32 和 W95 等。这些病毒的一般公有的特性是可以感染 Windows 操作系统的 *.exe 和 *.dll 文件，并通过这些文件进行传播。如 CIH（Win32.cih）、FUNLOVE（Win32.Funlove）。

（2）网络蠕虫。网络蠕虫的前缀是 Worm。这种恶意程序的公有特性是通过网络或者系统漏洞进行传播，很大部分的网络蠕虫都有向外发送带毒邮件、阻塞网络的特性。如 Worm.Sasser.f、Worm.Blaster.g。

（3）特洛伊木马程序。木马病毒的前缀是 Trojan。木马病毒的公有特性是通过网络或者系统漏洞进入用户的系统并隐藏，然后向外界泄露用户的信息。如 Trojan.QQ3344、Backdoor.NeThief.10、Hack.Nether.Client、Backdoor.Nethief.yi、Backdoor.NeThief.10.a 和 Trojan.Pwd.Oicq.c.enc。

（4）脚本病毒。脚本病毒的前缀是 Script。脚本病毒的公有特性是使用脚本语言编写，通过网页进行传播的病毒，如红色代码（Script.Redlof）。脚本病毒还会有如下前缀：VBS、JS（表明是何种脚本编写的），如欢乐时光（VBS.Happytime）、十四日（Js.Fortnight.c.s）等。

（5）宏病毒。其实宏病毒也是脚本病毒的一种，由于它的特殊性，因此在这里单独算成一类。宏病毒的前缀是 Macro，第二前缀是 Word、Word 97、Excel、Excel 97（也许还有别的）其中之一。凡是只感染 Word97 及以前版本 Word 文档的病毒采用 Word 97 作为第二前缀，格式是 Macro.Word 97；凡是只感染 Word 97 以后版本 Word 文档的病毒采用 Word 做为第二前缀，格式是 Macro.Word；凡是只感染 Excel 97 及以前版本 Excel 文档的病毒采用 Excel 97 作为第二前缀，格式是 Macro.Excel 97；凡是只感染 Excel 97 以后版本 Excel 文档的病毒采用 Excel 作为第二前缀，格式是 Macro.Excel，依此类推。该类病毒的公有特性是能感染 Office 系列文档，然后通过 Office 通用模板进行传播，如著名的美丽莎（Macro.Melissa）。

（6）后门程序。后门程序的前缀是 Backdoor。该类程序的公有特性是通过网络传播，给系统开后门，给用户计算机带来安全隐患。如 Backdoor.Agobot.frt、Backdoor.Hac-Def.ays。

（7）病毒种植程序病毒。这类病毒的公有特性是运行时会从体内释放出一个或几个新的病毒到系统目录下，由释放出来的新病毒产生破坏。如冰河播种者（Dropper.BingHe2.2C）、MSN 射手（Dropper.Worm.Smibag）等。

（8）破坏性程序病毒。破坏性程序病毒的前缀是 Harm。这类病毒的公有特性是本身具有好看的图标来诱惑用户点击，当用户点击这类病毒时，病毒便会直接对用户计算机产生破坏。如格式化 C 盘（Harm.formatC.f）、杀手命令（Harm.Command.Killer）等。

（9）玩笑病毒。玩笑病毒的前缀是 Joke。也称恶作剧病毒。这类病毒的公有特性是本身具有好看的图标来诱惑用户点击，当用户点击这类病毒时，病毒会做出各种破坏操作来吓唬用户，其实病毒并没有对用户计算机进行任何破坏。如女鬼（Joke.Girlghost）

病毒。

（10）捆绑机病毒。捆绑机病毒的前缀是 Binder。这类病毒的公有特性是病毒作者会使用特定的捆绑程序将病毒与一些应用程序如 QQ、IE 捆绑起来，表面上看是一个正常的文件，当用户运行这些捆绑病毒时，会表面上运行这些应用程序，然后隐藏运行捆绑在一起的病毒，从而给用户造成危害。如捆绑 QQ（Binder.QQPass.QQBin）、系统杀手（Binder.killsys）等。

以上为比较常见的病毒前缀，有时还会看到一些其他的病毒后缀，这里简单提一下。

- DoS：会针对某台主机或者服务器进行 DoS 攻击。
- Exploit：会自动通过溢出对方或者自己的系统漏洞来传播自身，或者它本身就是一个用于 Hacking 的溢出工具。
- HackTool：黑客工具，也许本身并不破坏你的机子，但是会被别人加以利用来用你做替身去破坏别人。

4.1.3　典型的恶意代码

1．计算机病毒

计算机病毒是目前恶意代码中数量及种类最多的程序之一，计算机病毒与其他恶意代码最大的区别在于计算机病毒是可以传播的，且需要用户操作来触发执行。

1）计算机病毒的特点

计算机病毒的特征可以归纳为传染性、程序性、破坏性、非授权性、隐蔽性、潜伏性、可触发性和不可预见性。

（1）传播性。传播性是指计算机病毒具有把自身复制到其他程序的能力。是否具有传播性是判别一个程序是否为计算机病毒的最重要条件之一。

（2）程序性。计算机病毒是计算机程序，需要依赖于特定的程序环境。

（3）破坏性。病毒一旦侵入系统都会对系统的运行造成不同程度的影响。该部分特性与病毒作者编写病毒的目的有很大关系。例如，有些病毒用来盗取用户各类账号密码，有些病毒则用来将被控制主机作为僵尸程序以对指定目标发起拒绝服务攻击等。

（4）非授权性。一般正常的程序是由用户调用，再由系统分配资源，完成用户交给的任务。其目的对用户是可见的、透明的。而病毒具有正常程序的一切特性，它隐藏在正常程序中。当用户调用正常程序时，窃取到系统的控制权，先于正常程序执行，病毒的动作对用户是未知的，是未经用户允许的。病毒的执行对系统而言是未授权的。

（5）隐蔽性。

① 病毒程序代码简洁短小。

② 其附着在正常程序或磁盘较隐蔽的地方，也有个别以隐含文件形式出现，或者病毒本身会使用 Rootkit 技术对自身的痕迹进行隐藏。

③ 病毒取得系统控制权后，系统仍能正常运行，使用户不会感到任何异常。

（6）潜伏性。大部分病毒感染系统后不会马上发作，它可长期隐藏在系统中，只有在满足其特定条件时才启动其表现模块。

（7）可触发性。病毒一般都有一个或者几个触发条件。如果满足其触发条件，激活病毒的传染机制进行感染，或者激活病毒的表现部分或破坏部分。

（8）不可预见性。从对病毒的检测方面来看，病毒还有不可预见性。

2）计算机病毒的生命周期

一个计算机病毒程序的整个生命周期一般由如下 4 个阶段组成。

（1）潜伏阶段：该阶段病毒处于休眠状态，这些病毒最终会被某些条件（如日期、某特定程序或特定文件的出现、内存的容量超过一定范围）所激活。当然，并不是所有的病毒都经历此阶段。

（2）传播阶段：病毒程序将自身复制到其他程序或磁盘的某个区域上，或者传播到其他计算机中，每个被感染的程序或者计算机又因此包含了病毒的复制品，从而也就进入了传播阶段。

（3）触发阶段：病毒在被激活后，会执行某一特定功能从而达到某种目的。和处于潜伏期的病毒一样，触发阶段病毒的触发条件是一些系统事件，例如可以为病毒复制自身的次数，也可以是系统日期或者时间，如 CIH1.2 病毒于 4 月 26 日爆发。

（4）发作阶段：病毒在触发条件成熟时，即可在系统中发作。由病毒发作体现出来的破坏程度是不同的，有些是无害的，有些则给系统带来巨大危害。

3）计算机病毒的传播途径

随着网络技术的快速发展和计算机的广泛普及，计算机病毒的传播途径也越来越多。

计算机病毒的传播途径可以大致分为如下几类。

（1）通过软盘、光盘传播。

软盘作为最常用的交换媒介，在早期的计算机应用中对病毒的传播产生了重要的作用，因为那时计算机应用比较简单，可执行文件和数据文件系统都较小，许多执行文件都需要通过软盘相互复制、安装，这样就能通过软盘传播文件型病毒。另外，在通过软盘列目录或引导机器时，引导区病毒会在软盘与硬盘引导区内互相感染。因此，软盘也成了计算机病毒主要的寄生“温床”。软磁盘在 21 世纪之前使用比较频繁，这也是之前计算机病毒传播的最主要方式。

光盘因为容量大，可以存储大量的可执行文件，光盘成为目前软件和数据交换最主要的方式之一。而大量的病毒就有可能藏身于光盘中。对于只读式光盘，由于不能进行写操作，因此光盘上的病毒不能清除。在以谋利为目的非法盗版软件制作过程中，不可能为病毒防护担负专门责任，也决不会有真正可靠的技术保障避免病毒的侵入、传染、流行和扩散。当前，盗版光盘的泛滥给病毒的传播带来了极大的便利，甚至有些光盘上的反病毒软件本身就带有病毒，这就给本来“干净”的计算机带来了灾难。

另外，用户自己在进行光盘刻录备份数据时，也可能将被感染计算机病毒的程序刻录备份。

（2）通过移动存储设备传播。

随着网络视频、音乐、手机与计算机文件交换发展，U 盘、MP3 等可移动介质被黑客广泛利用来传播病毒。只要 U 盘在中毒计算机上使用过，就会被植入病毒，当它被拿到别的计算机上使用时，就会感染更多的机器。

移动存储设备是目前计算机病毒最流行的传播方式，绝大部分计算机病毒都利用移动存储设备进行传播。

目前，U 盘病毒传播的方式主要有以下几种。

① 通过 autorun.inf 文件进行传播（目前 U 盘病毒最普遍的传播方式）。

② 伪装成其他文件。病毒把 U 盘下所有文件夹隐藏，并把自己复制成与原文件夹名称相同的具有文件夹图标的文件，当你点击时病毒会执行自身并且打开隐藏的该名称的文件夹。

③ 通过可执行文件感染传播，很古老的一种传播手段，但是依然有效。

作为移动存储介质使用最频繁的场所，打印社、计算机机房和多媒体教室目前已经成为计算机病毒传播的最主要场所。

目前通过 U 盘传播的病毒占据总病毒数的比例，在 2006 年还不足 10%，到 2007 年则上升到 32%左右。而且，该传播方式往往和其他方式结合，以取得更好的传播效果。

有时，带病毒的硬盘会被在本地或移到其他地方使用甚至维修等，这就会传染干净的软盘或者感染其他硬盘并扩散病毒。

（3）通过网络传播。

计算机网络是目前计算机病毒急速增长、种类快速增加的直接推动力，几乎任何一种网络应用都可能成为计算机病毒传播的有效渠道。计算机病毒常见的网络传播方式如下。

① 通过局域网传播。局域网是由相互连接的一组计算机组成的，这是数据共享和相互协作的需要。组成网络的每一台计算机都能连接到其他计算机，数据也能从一台计算机发送到其他计算机上。如果发送的数据感染了计算机病毒，接收方的计算机将自动被感染，因此，有可能在很短的时间内感染整个网络中的计算机。局域网络技术的应用为企业的发展作出巨大贡献，同时也为计算机病毒的迅速传播铺平了道路。同时，由于系统漏洞所产生的安全隐患也会使病毒在局域网中传播。

② 通过穷举局域网其他计算机的管理员弱口令。由于部分计算机用户没有为计算机管理员账户设置复杂的密码，这使得通过弱口令猜解的计算机病毒得到广泛传播。例如，2003 年 3 月爆发的“口令蠕虫”使用了这种传播方式。

③ 电子邮件（如邮件附件，或者带恶意程序的邮件正文等）。Outlook 以及 Outlook Express 是最常用的邮件客户端软件，也是非常容易受到邮件病毒攻击的软件。由于这类

软件有两个重要漏洞：预览漏洞和执行漏洞，因此产生了大量利用这两个漏洞的病毒。利用预览漏洞编写的病毒，用户只要一点击该病毒邮件，病毒就会自动执行破坏代码，使用户防不胜防。利用执行漏洞编写的病毒，它的带毒邮件会有一个特点，就是邮件很大但用户却看不到附件，原因是病毒利用邮件编码功能将自身以媒体形式隐藏在邮件的正文中，只要用户打开该邮件，病毒就会自动还原成病毒，继而对用户计算机进行破坏。如“欢乐时光（VBS.Happytime）”病毒会将自己伪装成信纸，然后附加到邮件的正文中四处传播；而“求职信（Worm.Klez）”病毒则是利用邮件预览漏洞进行传播的。

④ 各类即时通信软件（如 QQ、MSN 和 Skype 等）。即时通信（Instant Messenger，IM）软件可以说是目前我国上网用户使用率最高的软件，它已经从原来纯娱乐休闲工具变成生活工作的必备利器。由于用户数量众多，再加上即时通信软件本身的安全缺陷，例如内建有联系人清单，使得病毒可以方便地获取传播目标，这些特性都能被病毒利用来传播自身，导致其成为病毒的攻击目标。对即时通信软件形成安全隐患的病毒还正在陆续发现中，并有越演越烈的态势。

利用发送窗口中的超链接功能进行传播是即时通信软件的最主要传播方式之一，超链接功能即当用户收到好友发来的一个网址时，只要单击该网址就能直接进入该网页。由于该功能的方便性，被很多病毒利用，病毒运行时会利用聊天窗口向所有在线好友发送一个病毒网址的活链接，当好友误以为是有用网址单击时就会中毒，从而使病毒得到广泛传播。例如，大规模泛滥的“QQ 尾巴（Trojan.QQ3344.s）”病毒运行时会向正在聊天的 QQ 用户发送消息，收到消息的 QQ 好友如果单击该链接地址，就会中毒，然后继续感染其他正在 QQ 上聊天的 QQ 好友。

⑤ 利用各类浏览器漏洞（如 IE、Firefox 和 Opera 等）的网页挂马。IE 浏览器是我们使用最多的浏览器，它也存在许多安全漏洞并成为病毒的攻击对象。最常见的病毒攻击方式是利用脚本执行漏洞。该漏洞会在用户浏览网页时自动执行网页中的有害脚本程序，或者自动下载一些有害的病毒，从而对用户的计算机造成破坏。如“极限女孩”病毒，它内嵌在网页中，当用户在不知情的情况下打开含有该病毒的网页时，病毒就会修改用户的 IE 默认首页、在桌面上建立大量的色情网站链接，影响用户正常使用计算机。

2007 年，包括网页挂马（木马病毒）、钓鱼网站和流氓网站等成为新的最大的威胁来源。通过在网页内嵌入木马病毒进行传播，已经成为黑客传播病毒的主要渠道，而国内大量存在安全缺陷的网站，则给黑客提供了便利条件。甚至一些大型站点和门户网站被黑客入侵之后，也会被挂上网页木马。另外，各类黄色站点、视频聊天等网站本身就包含大量恶意网页。

现在黑客们往往会利用社会热点来实施网页挂马攻击，例如电影《色戒》、《贝布托夫人遇刺》等，都曾被黑客利用来传播病毒。由于通过“网页挂马”可以快速地批量入侵大量计算机，获取经济利益，因此“网页挂马”成为黑客常用的攻击手段。

⑥ P2P 下载渠道（如 BT、电驴等）。P2P 软件是点对点的传输通信工具，只要使用

同一个 P2P 软件，用户之间就可以直接进行交流、聊天和交换文件等。随着 P2P 软件使用范围的普及，有越来越多的病毒开始盯上这类软件。大多数攻击 P2P 软件的病毒都是利用自动配置脚本和共享目录进行传播。病毒感染用户计算机时就会查找这些 P2P 软件所在的目录，然后将自身加入到脚本配置文件中，由该配置文件自动将病毒传播出去。或者病毒会将自己复制到 P2P 软件的共享目录中去，并由 P2P 软件的其他用户主动运行病毒，从而造成病毒传播。像“泡沫人（Worm.p2p.fizzer）”病毒就是一个通过 P2P 软件的共享目录进行传播的恶性病毒，病毒泛滥时会造成网络阻塞。

⑦ 各类软件下载站点。目前，有一些个人用户构建软件下载站点，这些站点中有很大一部分软件都包含了计算机病毒。另外，某些大型的软件下载站点被黑客入侵之后，其正常软件也可能被感染或捆入计算机病毒，从而使得下载者的计算机感染。

⑧ 各类应用软件漏洞。很多流行的应用软件，包括迅雷、百度搜霸、Realplayer 和 Qvod 等都曾出现过安全漏洞。对于很多用户来讲，只要这些软件能够正常使用，就不会去升级新版本，这样使得很多用户的计算机都存在漏洞。这些用户去访问带毒网站时，很容易就会被感染。

⑨ 各类系统漏洞。漏洞是指操作系统中的某些程序中存在一些人为的逻辑错误，这些错误隐藏很深，一般是被一些程序员或编程爱好者在研究系统的过程中偶然发现的，这些发现的错误公布后很可能被一些黑客利用，于是这些能被利用的逻辑错误就成了漏洞。

目前，各类操作系统都不可避免地存在大量的安全问题和缺陷。例如，微软每个月第二个星期二都会公布 Windows 操作系统的一系列安全公告。这些安全漏洞都给计算机病毒传播特别是蠕虫的传播提供了绝佳的条件，特别是大量 0day 漏洞的出现，更是让广大用户苦不堪言。

Windows 系列操作系统之所以容易受到病毒攻击，主要是因为操作系统设计复杂，会出现大量的安全漏洞。如 2003 年 8 月份全球泛滥的“冲击波（Worm.Blaster）”病毒就是利用了系统的 RPC 缓冲区漏洞才得以大面积传播与泛滥。

据不完全统计，Windows NT 系列操作系统已存在有近千个已知的安全漏洞。而随着新操作系统的推出，新漏洞将会更多地被发现。

不过，相对来讲，目前修补系统漏洞的工具和技术都比较成熟，很多安全软件都提供了系统漏洞扫描和补丁修补安装的功能，如 360 安全卫士。

⑩ ARP 欺骗。ARP 地址解析协议是一种常用的网络协议，每台安装有 TCP/IP 协议的计算机里都有一个 ARP 缓存表，表里的 IP 地址与 MAC 地址一一对应，如果这个表被修改，则会出现网络无法连通，或者访问的网页被劫持。黑客利用 ARP 协议存在的缺陷，侵入某台计算机之后发送 ARP 欺骗攻击数据包，造成局域网内所有用户在访问网络时，收到的都是带毒的网页。

⑪ 无线设备传播。目前，这种传播途径随着手机功能性的开放和增值服务的拓展，

已经成为有必要加以防范的一种病毒传播途径。随着智能手机的普及，通过彩信、上网浏览与下载到手机中的程序越来越多，不可避免地会对手机安全产生隐患，手机病毒会成为新一轮计算机病毒危害的“源头”。手机，特别是智能手机和3G网络发展的同时，手机病毒的传播速度和危害程度也与日俱增。通过无线传播的趋势很有可能将会发展成为第二大病毒传播媒介，并很有可能与网络传播造成同等的危害。

4）计算机病毒的多种状态

计算机病毒在传播中存在静态和动态两种状态，这里用“静态病毒”和“动态病毒”来表示处于这两种状态的病毒。

（1）静态病毒：是指存在于辅助存储介质上的计算机病毒。因为程序只有被操作系统加载才能进入内存执行，静态病毒未被加载，所以不存在计算机内存，更没有被系统执行。因此，静态病毒不能产生传染和破坏作用。有时，这种休眠状态的病毒被称为潜伏病毒。另外，某种病毒存在于不可执行它的系统中，该病毒就会处于一种特别的睡眠状态。对于处于静态的计算机病毒来说，其在计算机中的存在形式便是文件或者保存在扇区中的病毒代码。

（2）动态病毒：是指进入了计算机内存的计算机病毒，它必定是随病毒宿主的运行或者系统的启动机制而运行，如使用寄生了病毒的软、硬盘启动计算机，或执行被感染病毒的程序文件时进入内存，就会使计算机病毒处于动态运行状态。动态病毒本身处于运行状态，或通过截留盗用某些系统中断或设备驱动程序头能力及获得运行权（系统控制权）。计算机病毒的传染和破坏功能必须由计算机病毒在动态执行时调用触发，计算机病毒的传染和破坏作用都是动态病毒产生的。

内存中的动态病毒又有两种状态：能激活态和激活态。

① 能激活态：当内存中的病毒代码能够被系统的正常运行机制所执行时，动态病毒就处于能激活态。修改中断向量表的动态病毒能在系统调用病毒修改中断时被执行；修改设备驱动程序头的动态病毒能在系统使用该设备驱动程序时被执行。获得部分的系统控制权。

② 激活态：系统正在执行病毒代码时，动态病毒就处于激活态。病毒处于激活态时，不一定进行感染和破坏；但进行感染和破坏时，必然处于激活态。处于激活态的动态病毒拥有系统控制权，它监视系统的运行，一旦满足传染或破坏条件，就调用病毒代码中的传染破坏模块，扩散病毒或破坏系统。获得了全部系统控制权。能激活态的病毒能借助截留盗用系统正常运行机制转变为激活态病毒，获得系统控制权。

内存中的病毒还有一种较为特殊的状态——失活态，这种状态在一般情况下不会出现。它的出现一般是由于用户对病毒的干预（用杀毒软件或手工方法）。内存中的病毒代码不能被系统的正常运行机制执行，此时，内存中的病毒就处于失活态。处于失活态的内存病毒不可能进行传染或破坏。它与静态病毒的不同仅在于病毒代码在内存中，但得

不到执行。

5）Windows 环境下的几类常见计算机病毒

（1）Windows PE 病毒。

PE（Portable Executable，可移植的执行体）是 Win32 环境自身所带的执行体文件格式，它的一些特性继承自 UNIX 的 Coff（common object file format）文件格式。

PE 病毒是指所有感染 Windows 下 PE 文件格式文件的病毒。PE 病毒在进行文件感染或网络传播时存在多种感染方式。

① 传统感染。该类病毒最具技术性，病毒编写者通常需要对 PE 文件格式有比较深入的了解。该类病毒感染的原理是将病毒代码写入到目标宿主程序体内，然后修改目标宿主程序的文件头或者部分程序代码，使得宿主程序在运行时可以调用病毒代码的执行。这类病毒感染目标程序之后通常不会改变目标程序的图标，如果采用空隙式感染则不会增加目标程序的大小（如 CIH 病毒）。

这类病毒编写起来难度较大，写入到目标宿主程序体内的病毒代码自身要解决变量重新定位、自己搜索 API 函数地址等关键技术。通常这类病毒是使用 Win32 汇编编写的。这类计算机病毒在进行病毒清除时也比较困难。

② 捆绑式感染。该类计算机病毒在感染宿主程序时，会将自身整体直接或者进行压缩之后放入到目标宿主程序之中，或者将自身代码覆盖到目标宿主程序最前面，同时将目标宿主程序直接或者进行压缩后保存在病毒程序之后。这样，当目标宿主程序运行时，实际上执行的是计算机病毒程序，为了保证目标程序也可以正常执行，该类计算机病毒会将原始目标程序解压释放然后执行。

当然，这类病毒在感染时需要对目标程序的图标进行提取替换，否则目标程序的图标就会发生改变。例如，熊猫烧香病毒便是这种感染方式，且被感染之后的 PE 文件图标都是一个熊猫图案。

这类计算机病毒在清除时的难度较前一种感染方式较小。

③ 复制性传播。这类计算机病毒本身不对任何 PE 文件进行感染，其通常在目标计算机中保存几个病毒文件。由于不感染任何文件，因此这类病毒程序必须在操作系统中写入自启动项，以便于系统重新启动之后这些病毒程序可以获得控制权。这类计算机病毒由于不感染本地主机中的文件，其在进行传播时通常采用可移动存储介质或者网络交互方式进行传播。

④ 覆盖式传播。这类计算机病毒直接对目标 PE 文件进行覆盖，如“小浩”病毒。这类计算机病毒没有什么技术性可言，感染该类计算机病毒之后，原有的被感染文件数据全部或者部分丢失。在对这类计算机病毒进行清除时，直接删除掉病毒体文件即可。

（2）脚本病毒。

脚本病毒是指利用.asp、.htm、.html、.vbs 和.js 等类型的文件进行传播的基于 VB Script 和 Java Script 脚本语言并由 WSH（Windows 脚本宿主）解释执行的一类病毒。任何语言

都是可以编写病毒的，而用脚本编写病毒则尤为简单，并且编出的病毒具有传播快，破坏力大的特点。

脚本病毒种类比较多，比较常见的是 VBS 脚本病毒。

VBS 病毒是用 VBScript 编写而成，该脚本语言功能非常强大，它们利用 Windows 系统的开放性特点，通过调用一些现成的 Windows 对象、组件，可以直接对文件系统、注册表等进行控制。可以说，病毒实际上就是一种构思，但是这种构思在用 VBS 实现时变得极其容易。

脚本病毒具备如下特点。

① 编写简单。一个对病毒一无所知的计算机使用者也可以在很短的时间里编出一个新型病毒来。

② 破坏力大。其破坏力不仅表现在对文件系统及机器性能的破坏，还可以使邮件服务器崩溃，网络发生严重阻塞。

③ 感染力强。由于脚本是直接解释执行，并且它不需要像 PE 病毒那样做复杂的 PE 文件字段处理，因此这类病毒可以直接通过自我复制的方式感染其他同类文件，并且自我的异常处理变得非常容易。

④ 传播范围大。这类病毒还可以通过 HTM 和 ASP 等网页文件、E-mail 附件、KaZaA 等网络共享工具和 IRC 传播，可以在很短时间内传遍世界各地。

⑤ 病毒源码容易被获取，变种多。由于 VBS 病毒解释执行，其源代码可读性非常强，即使病毒源码经过加密处理后，其源代码的获取还是比较简单。因此，这类病毒变种比较多，稍微改变一下病毒的结构，或者修改一下特征值，很多杀毒软件可能就无能为力了。

⑥ 欺骗性强。脚本病毒为了得到运行机会，往往会采用各种让用户不大注意的手段，例如，邮件的附件名采用双后缀，如.jpg.vbs。由于系统默认不显示后缀，这样，用户看到这个文件时，就会认为它是一个 jpg 图片文件。

⑦ 使病毒生产机实现起来非常容易。所谓病毒生产机，就是可以按照用户的要求进行配置以生成特定病毒的机器（当然，这里指的是程序）。目前的病毒生产机之所以大多数都为脚本病毒生产机，其中最重要的一点还是因为脚本采用解释执行的方式，实现起来非常容易。

（3）宏病毒。

宏是微软公司出品的 Office 软件包中所包含的一项特殊功能。微软设计此项功能的主要目的是给用户自动执行一些重复性的工作提供方便。它利用简单的语法，把常用的动作写成宏，用户工作时，就可以直接利用事先编好的宏自动运行，以完成某项特定的任务，而不必反复重复相同的动作。宏是一段类似批处理命令的多行代码的集合。在 Word 中可以通过按 Alt+F8 组合键查看存在的宏，通过按 Alt+F11 组合键调用宏编辑窗口。

宏病毒是使用宏语言编写的程序，可以在一些数据处理系统中运行（主要是微软的办公软件系统，字处理、电子数据表和其他 Office 程序中），其存在于字处理文档、数据表格、数据库和演示文档等数据文件中，利用宏语言的功能将自己复制并且繁殖到其他数据文档里。宏病毒本质上是利用宏语言（如 VBA）进行编写的一些宏，不过这些宏的应用不是为了给人们的工作提供便利，而是会破坏文档，使人们的工作遭受损失。

2．网络蠕虫

网络蠕虫由于不需要用户干预来触发，因而其传播速度要远远大于网络病毒。因而，其对网络性能产生的影响则更为显著和严重。

表 4-1 列举了曾经出现过的著名蠕虫及它们所利用的具体漏洞和具体爆发时间。

表 4-1　几个著名蠕虫

蠕 虫 名 称	所利用的具体漏洞	爆 发 时 间
Slammer	MS02-039	2003.1.25
Blaster	MS03-026	2003.07.11
Sasser	MS04-011	2004.05.01
Zotob	MS05-039	2005.08.14

网络蠕虫可以独立运行，并能把自身的一个包含所有功能的版本传播到另外的计算机上。

1）计算机病毒与蠕虫的区别

计算机病毒和网络蠕虫都具有传播性和破坏性，这导致两者之间是非常难区分的。表 4-2 给出病毒和蠕虫的一些差别：

表 4-2　病毒和蠕虫的区别

	病　　毒	蠕　　虫
存在形式	寄生	独立个体
复制机制	插入到寄主程序（文件）中	自身的复制
传染机制	宿主程序运行	系统存在漏洞
搜索机制	针对本地文件	网络上的其他计算机
触发机制	计算机使用者	程序自身
影响重点	文件系统	网络，系统性能
计算机使用者角色	病毒传播中的关键环节	无关
防治措施	从宿主文件中摘除	为系统打补丁
对抗主体	计算机使用者，反病毒厂商	系统提供商，网络管理人员

通过对多个蠕虫程序的分析，通常情况下可以粗略地把蠕虫程序或代码的功能分为基本功能模块和扩展功模块。

2）基本功能模块

基本功能模块是几乎每一个蠕虫都应该具备的模块，这些模块构成了网络蠕虫进行传播不可缺少的最基本的功能。

（1）目标搜索或生成模块。本模块主要用来搜索可被感染的目标主机。此部分通常存活主机扫描及漏洞扫描模块。当然，有些蠕虫自身并没有存活主机扫描模块，而只是随机产生目标 IP 地址，如 SQL Slammer。

（2）攻击模块。在被感染的计算机上建立控制通道，该模块通常需要利用目标主机的缺陷或漏洞来获取对目标主机的控制权。这也是蠕虫赖以生存的关键手段。从单次攻击来讲，该模块和 Exploit 程序发起一次攻击效果是一致的。

（3）传输模块。蠕虫的传输通常包括两种方式：直接在攻击模块中发送带蠕虫全部数据的数据包，或者在获得对方主机的控制权之后下载或者接收攻击计算机发送的蠕虫文件。例如，SQL Slammer 采用了第一种方式，而冲击波和振荡波则采用了后面的方式。

3）扩展功能模块

扩展功能模块并不是每一个蠕虫都必须具有的模块，这通常与蠕虫作者编写蠕虫的目的有很大关系。扩展功能模块本身与其他恶意代码的功能模块在技术上没有很大区别。

（1）主机驻留模块。在目标主机硬盘中建立自身的多个副本，并设置自启动选项，以长期驻留在目标主机中。这种驻留方式与其他类型的恶意代码是一致的。当然，有的网络蠕虫并不驻留在主机硬盘之中，例如，红色代码和 Slammer 蠕虫仅驻留在内存之中，在关机之后该蠕虫就会自动消失。

（2）隐藏模块。对蠕虫产生的各类文件和对象进行隐藏。

（3）破坏模块。摧毁或破坏被感染计算机，或在被感染计算机上留下后门程序等。

（4）通信模块。蠕虫之间或者蠕虫同黑客之间进行交流的模块。

（5）控制模块。用来调整蠕虫行为，更新其他功能模块，控制被感染计算机。

3．特洛伊木马

计算机领域的“特洛伊木马（Trojan）”，是指附着在应用程序中或者单独存在的一些恶意程序，它可以利用网络远程控制网络另一端的安装有服务端程序的主机，实现对被植入了木马程序的计算机的控制，或者窃取被植入了木马程序的计算机上的机密资料。

同其他的黑客工具一样，木马程序具有隐蔽性和非授权性。所谓隐蔽性，是指木马设计者为了防止木马程序被发现，会尽可能地采用各种隐藏手段，这样即使被发现，也往往因为无法具体定位而无法清除。所谓非授权性，是指木马程序的控制端与服务端连接后，具有服务端程序窃取的各种权限，可以由服务端接收客户端计算机发送来的命令，并在服务端计算机上执行，包括修改或删除文件、控制计算机的键盘鼠标、修改注册表、按木马控制者的意愿重启被攻击的计算机、截取服务端的屏幕内容等。

从本质上讲，木马是一种基于远程控制的工具，类似于远端管理软件，如 PC-Anywhere。木马与一般远程管理软件的区别在于木马具有隐蔽性和非授权性的特点。

木马程序一般利用 TCP/IP 协议，采用 C/S 结构，分为客户端（也称控制端）和服务器端（也称被控制端）两个部分。木马的两端程序通常运行于网络上不同的两台计算机。服务器端程序运行于被攻击的计算机上，而客户端程序在控制者的计算机上运行。客户端程序可以同时向多个服务端程序发送命令以同时控制这些计算机。客户端程序一般提供友好的操作界面，以便于用户的操作，其功能比较丰富。

4. 后门

后门是指那些绕过安全性控制而获取对程序或系统访问权的程序。早期的计算机黑客，在成功获得远程系统的控制权后，希望能有一种技术使得他们在任意时间都可以再次进入远程系统，于是后门程序就出现了。后门是一种登录系统的方法，它不仅绕过系统已有的安全设置，而且还能挫败系统上各种增强的安全设置。用很简单的一句话来概括它：后门就是留在计算机系统中，供特殊使用者通过某种特殊方式控制计算机系统的途径。

在软件的开发阶段，程序员常常会在软件内创建后门程序以便可以修改程序设计中的缺陷。但是，如果这些后门被其他人知道，或是在发布软件之前没有删除后门程序，那么它就存在安全隐患，容易被黑客当成漏洞进行攻击。传统意义上的后门程序往往只是能够让黑客获得一个 SHELL，通过 SHELL 进而进行一些远程控制操作。

后门程序跟我们通常所说的“木马”有联系也有区别。联系在于，都是隐藏在用户系统中向外发送信息，而且本身具有一定权限，以便控制者对被控制主机的控制；区别在于，木马是一个非常完整的工具集合，而后门大多数则体积较小且功能都很单一，所以木马提供的功能远远超过后门程序。当然，随着后门技术的发展，后门程序的功能也开始逐渐完善，所以目前的木马和后门有时候很难具体区分开来。当然，有的观点也认为，木马和后门最大的区别在于木马程序本身有很强的隐蔽性和迷惑性，其通常隐藏在某些看起来具有正常功能的程序之中。如果将后门程序伪装成正常程序，那么该程序也就成了木马。

5. 网页木马

网页木马实际上是经过黑客精心制作的 HTML 网页文件，用户一旦访问了该网页就会中木马病毒。各类浏览器都存在一些安全漏洞（图 4-3 描述了 IE 浏览器面临的几个安全漏洞信息），嵌入在这个网页文件中的脚本恰如其分地利用了浏览器的漏洞，让浏览器在后台自动下载并执行黑客放置在网络上的木马。也就是说，只要用户访问了该网页文件，浏览器就会自动下载木马到本地，并自动运行（安装）下载到本地计算机上的木马，整个过程都在后台运行。

6. Rootkit 程序

Rootkit 所采用的大部分技术和技巧都用于在计算机上隐藏代码和数据。例如，许多 Rootkit 可以隐藏文件和目录。Rootkit 的其他特性通常用于远程访问和窃听，例如，用于嗅探网络上的报文。当这些特性结合起来后，它们会给系统带来严重的安全隐患。

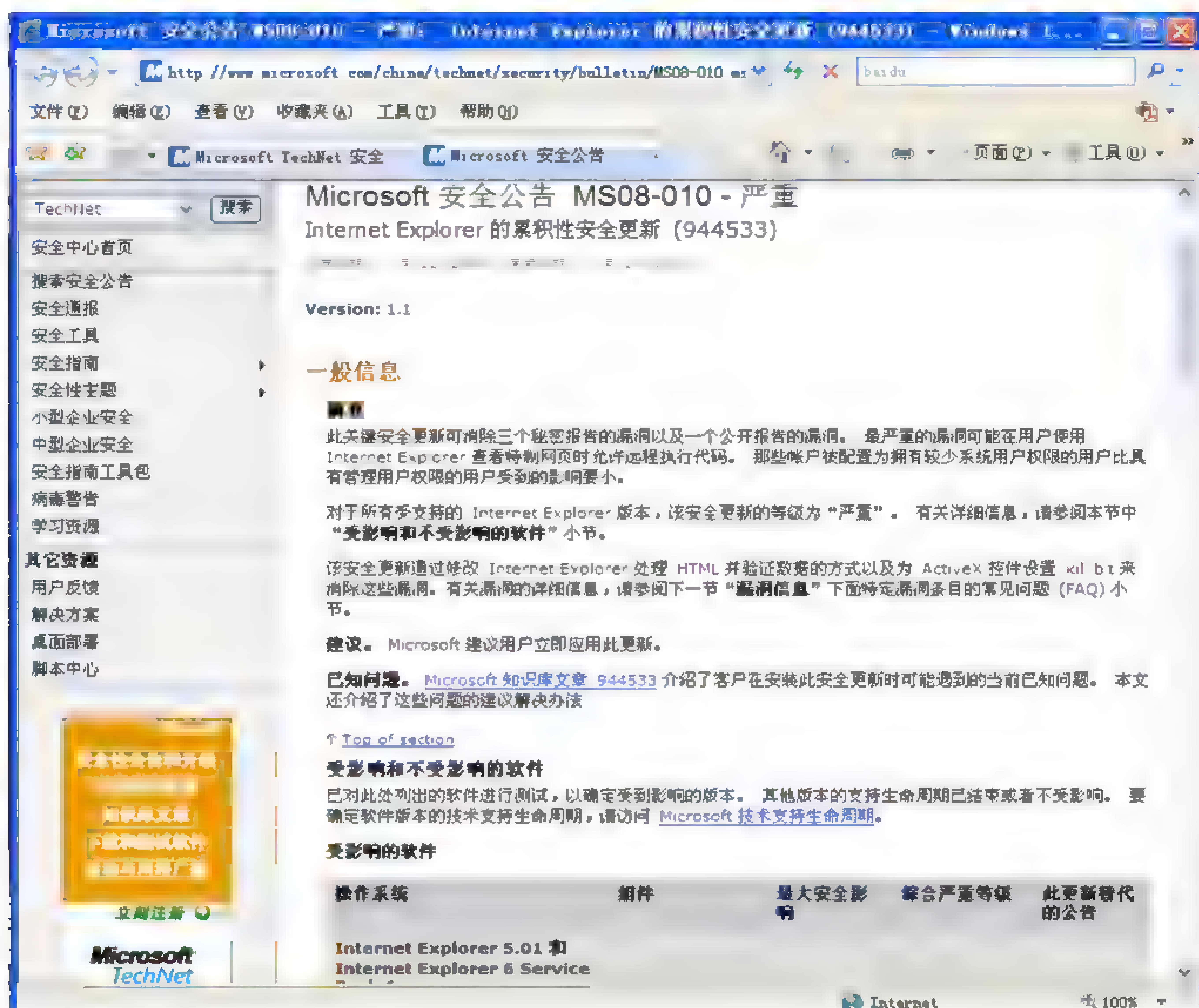


图 4-3 微软安全公告 MS08-010：IE 的累积性安全更新

Rootkit 并非天生邪恶，也并不总是被黑客所使用。Rootkit 只是一种技术，美好或邪恶的意图取决于使用它们的人。大量合法的商用程序提供了远程管理，甚至窃听功能。有些程序甚至使用潜行技术。这些程序在许多方面都可称作 Rootkit。法律实施领域可以使用术语 Rootkit 来指代被核准的后门程序——根据国家法律（可能通过法院指令）允许在目标上安装它们。大型公司也使用 Rootkit 技术来监测和实施自己的计算机使用规范。

只有当希望维持对系统的访问时，Rootkit 才发挥作用。若要完成的全部功能只是窃取信息然后离开，则没有必要留下 Rootkit。事实上，留下 Rootkit 总是存在着被检测发现的风险。若窃取了信息并将系统清理干净，就可以不留下任何操作痕迹。

可以把 Rootkit 理解成一个利用很多技术来潜伏在目标系统中的一个后门，并且包含了一个功能比较多的程序包，例如有清除日志、添加用户、提供 cmdshell 和添加删除启动服务等功能。当然，它的设计者也要用一些技术来隐藏程序，以确保不被发现。目前 RootKit 常见的隐藏范围包括隐藏进程、文件、端口、网络连接、句柄、注册表的项

或键值等。总之，Rootkit 的设计者总是绞尽脑汁利用各种技术以避免自身程序被发现。

Rootkits 主要分为两大类：用户态和内核态。用户态 Rootkit 通常是进程注入式 Rootkits，而内核态则多为驱动级 Rootkits。

第一种 Rootkits 技术通常通过释放动态链接库（DLL）文件，并将它们注入到其他软件及系统进程中运行，通过 HOOK 方式对消息进行拦截，阻止 Windows 及应用程序对被保护的文件进行访问。

第二种 Rootkits 技术较为复杂，其通过在 Windows 启动时加载 Rootkits 驱动程序，获取对 Windows 的控制权。当程序（Windows 及杀毒软件等）通过系统 API 及 NTAPI 访问文件系统时进行监视，一旦发现程序访问被 Rootkits 保护的文件时返回一个虚假的结果，从而达到隐藏或锁定文件的目的。

7．Exploit 与 ShellCode

Exploit 是一个小程序，通过使用该程序可以触发一个软件漏洞并被攻击者所利用。它是一种自动检测漏洞并能在大多数情况下通过运行代码来尝试利用漏洞的程序。它通常包含两个主要部分：用来触发并利用对方系统漏洞的代码和另外一段被称为 ShellCode 的代码。Exploit 又可以分为本地和远程两类。本地 Exploit 多用来提升权限，而远程 Exploit 多用于发动拒绝服务攻击或者获得目标主机的控制权。

通常，ShellCode 是用来执行 shell 的字节码。现在 ShellCode 有了更广泛的意思，可以定义一个成功 Exploit 在获得目标系统控制权之后所执行的功能代码。ShellCode 经常被大小的束缚所限制，例如受发送到脆弱应用程序的缓冲区的大小限制或者编码限制等。多数 ShellCode 的目的用于返回 shell 地址（又可以分为正向和反向 shell），但许多 ShellCode 也有其他的目的，如用来添加管理员账户、从远程 URL 下载并执行一个程序等。

有时，同一个漏洞在不同操作系统版本上的具体细节是不一样的，即使漏洞细节相同，但为了触发 ShellCode 获得控制权，其所选择的用来转跳到 ShellCode 的转跳语句也不一样。因此，对于同一个漏洞有时会出现多种针对不同操作系统环境的 Exploit。

8．黑客攻击程序

黑客攻击程序由于可能对计算机用户的计算机安全造成威胁，因此也经常被各大杀毒软件厂商纳入到病毒查杀范围之列。

9．流氓软件

流氓软件也称为灰色软件，是一种介于正常软件和恶意代码之间的软件。通常流氓软件是由合法的公司发布，主要用于商业目的。所以流氓软件一般不会对计算机用户的系统造成破坏，但是它会影响用户的正常使用，如广告软件不断地弹出广告，占用系统资源，更有甚者如间谍软件会记录用户的个人信息，造成严重的损失。

2006 年，中国互联网协会对流氓软件进行了定义。

流氓软件是指在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上安装运行、侵犯用户合法权益的软件，但已被我国现有法律法规规定的计算机病毒

除外。它具有如下特点。

（1）强制安装。是指在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上安装软件的行为。

（2）难以卸载。是指未提供通用的卸载方式，或在不受其他软件影响、人为破坏的情况下，卸载后仍活动的行为。

（3）浏览器劫持。是指未经用户许可，修改用户浏览器或其他相关设置，迫使用户访问特定网站或导致用户无法正常上网的行为。

（4）广告弹出。是指未明确提示用户或未经用户许可的情况下，利用安装在用户计算机或其他终端上的软件弹出广告的行为。

（5）恶意收集用户信息。是指未明确提示用户或未经用户许可，恶意收集用户信息的行为。

（6）恶意卸载。是指未明确提示用户、未经用户许可，或误导、欺骗用户卸载非恶意代码的行为。

（7）恶意捆绑。是指在软件中捆绑已被认定为恶意代码的行为。

（8）其他侵犯用户知情权、选择权的恶意行为。

4.1.4 典型反病毒技术和常用反病毒软件

1. 典型反病毒技术介绍

目前典型的反病毒技术有特征码技术、虚拟机技术、启发扫描技术、行为监控技术、主动防御技术和病毒疫苗等。

1）特征值查毒法

特征值扫描是目前国际上反病毒公司普遍采用的查毒技术。其核心是从病毒体中提取病毒特征值构成病毒特征库，杀毒软件将用户计算机中的文件或程序等目标，与病毒特征库中的特征值逐一比对，判断该目标是否被病毒感染。

目前绝大多数反病毒软件都采用了特征值查毒技术。这类反病毒软件不可缺少的两个部分是反病毒引擎和病毒特征库。反病毒引擎用来对疑似病毒样本文件进行扫描，其需要根据病毒特征库的特征条目来确定该疑似病毒样本文件是否包含了特定的计算机病毒。

目前，特征值检测技术已被公认是检测已知病毒最简单有效的方法。传统的特征串检测技术实现步骤如下。

（1）采集已知的病毒样本。即使是同一种病毒，当它感染不同的宿主时，就要采集多种样本。如果病毒既感染 COM 文件，又感染 EXE 文件以及引导区，那就要提取三个样本。

（2）在病毒样本中抽取特征串。抽取的特征串应比较特殊，不要与普通正常程序代码吻合。当抽取的特征串达到一定长度时，就能保证这种特殊性。抽取的特征串要有适

当长度，这保证了特征串的唯一性，同时查毒时又不需太大的空间和时间开销。

（3）将特征串纳入病毒特征数据库。

在实际应用中，反病毒软件使用反病毒引擎打开被检测文件，在文件中搜索，检查文件中是否含有病毒特征数据库中的病毒特征串。由于特征串与计算机病毒一一对应，如果发现病毒特征串，便可以判断被查文件中染有何种病毒。

特征值检测方法的优点是：检测准确、可识别病毒的名称、误报警率低，并且依据检测结果可做解毒处理。

其缺点如下。

（1）开销大、查杀速度慢。搜集已知病毒特征串的费用开销大。随着病毒种类的增多，获得分析样本的时间变长。另外，样本数急剧增加，目前各大反病毒公司的样本库记录都在几十万条以上，虽然样本数量和查杀速度不是线性关系，但进行病毒扫描的时间开销无疑将会逐渐增大。

（2）不能检查未知病毒和多态性病毒。特征值检测方法是不可能检测多态性病毒的，因为其代码不唯一。虽然目前有些反病毒厂商在提取特征码时提出了一些可以提取多态性病毒共同特征码的方法，但效果有限。

2）校验和技术

计算正常文件的内容和正常的系统扇区的校验和，将该校验和写入数据库中保存。在文件使用/系统启动过程中，检查文件现在内容的校验和与原来保存的校验和是否一致，因而可以发现文件/引导区是否感染，这种方法叫校验和检测技术。

校验和检测技术的优点是：方法简单、能发现未知病毒、被查文件的细微变化也能发现。其缺点是：必须预先记录正常文件的校验和、会误报警、不能识别病毒名称、不能对付隐蔽型病毒和效率低。

3）启发式扫描技术

启发性扫描主要是分析文件中的指令序列，根据统计知识判断该文件可能感染或者可能没有感染，从而有可能找到未知的病毒。因此，启发性扫描技术是一种概率方法，遵循概率理论的规律。

启发式扫描技术仍然是一种正在发展和不断完善的技术，但已经在大量优秀的反病毒软件中得到迅速的推广和应用。按照最保守的估计，一个精心设计的启发式扫描软件，在不依赖任何对病毒预先的学习和辅助信息，如特征值、校验和等的情况下，可以检查出许多未知的新病毒。当然，可能会出现一些虚报/谎报的情况。

4）虚拟机技术

多态性病毒每次感染都改变其病毒密钥，对付这种病毒，普通特征值检测方法失效。因为多态性病毒对其代码实施加密变换，而且每次传染使用不同密钥。把染毒文件中的病毒代码相互比较，也不易找出相同的可作为病毒特征的稳定特征值。虽然行为监测技术可以检测多态性病毒，但是在检测出病毒后，无法做病毒清除处理，因为不知该病毒

的具体特性。

一般而言，多态性病毒采用以下几种操作来不断交换自己。

（1）采用等价代码对原有代码进行替换。

（2）改变与执行次序无关的指令的次序。

（3）增加许多垃圾指令。

（4）对原有病毒代码进行压缩或加密。

但是，无论病毒如何变化、每一个多态病毒在其自身执行时都要对自身进行还原。为了检测多态性病毒，反病毒专家研制了一种新的检测方法——虚拟机技术。该技术也称为软件模拟法，它是一种软件分析器，用软件方法来模拟和分析程序的运行，而且程序的运行不会对系统起实际的作用（仅是“模拟”），因而不会对系统造成危害。其实质都是让病毒在虚拟的环境执行，从而让其原形毕露、无处遁形。

目前大多数反病毒软件都采用了虚拟机技术，反病毒软件开始运行时，使用特征值检测方法检测病毒。如果发现隐蔽式病毒或多态性病毒，启动软件模拟模块，监视病毒的运行，待病毒自身的加密代码解码后，再运用特征值检测方法来识别病毒的种类。

虚拟机技术在处理加密（encryption）、变换（mutation）、变形（polymorphic）病毒方面功能卓越，显示出该技术的优越性。变形病毒在传染的过程中不断地变化自己，所以提取它们的特征码非常困难。但是，任何变形病毒都会在执行时在内存中加密/还原成自身。虚拟机正是利用了这一点，根本不需要关心变形病毒的特征值，而是虚拟执行它们，这样就会将它们的外在变化全部去掉。显然，在这种情况下，病毒很容易被捕获。

虚拟机的引入使得反病毒软件从单纯的静态分析进入了动态和静态分析相结合的境界，极大地提高了已知病毒和未知病毒的检测水平，以相对比较少的代价获得了可观的突破。在今后相当长的一段时间内，虚拟机在合理的完整性、技术技巧等方面都会有相当的进展。

5）行为监控技术

病毒不论伪装得如何巧妙，它总是存在着一些和正常程序不同的行为。例如，病毒总要不断复制自己，否则它无法传染。再如，病毒总是要想方设法地掩盖自己的复制过程，如不改变自己所在文件的修改时间等。病毒的这些伪装行为做得越多，特征值检测技术越难以发现它们，由此反病毒专家提出了病毒行为监测技术，专门监测病毒行为。行为监控是指通过审查应用程序的操作来判断是否有恶意（病毒）倾向并向用户发出警告。这种技术能够有效防止病毒的传播，但也很容易将正常的升级程序、补丁程序误报为病毒。病毒程序的伪装行为越多，它们露出的马脚就越多，就越容易被监测到。

人们通过对病毒多年的观察、研究，发现病毒有一些共同行为。在正常应用程序中，这些行为比较罕见。这就是病毒的行为特性。

常见的病毒行为特性如下。

（1）引导型病毒必然截留盗用 INT 13H。

（2）高端内存驻留型病毒修改 DOS 系统数据区的内存总量。

（3）内存控制链驻留型病毒修改最后一个内存控制块（MCB）的段址。

（4）修改 INT 21H、INT 25H、INT 26H、INT 13H。

（5）修改 INT 24H DOS 严重错误中断。

（6）对可执行文件进行写操作（如修改 PE 文件图标资源、写入代码等）。

（7）不断搜索目标 PE 文件。

（8）释放可执行程序到系统目录并运行。

（9）在非代码节执行代码。

（10）写磁盘引导区。

（11）病毒程序与宿主程序的切换。

（12）从远程网站下载 PE 文件并运行。

以上就是病毒的行为特性，正常程序也可能具有此类行为，但是只有病毒才会同时具有数种病毒行为。利用此点，就可以对病毒实施监视，在病毒传染时发出报警。

但极少数正常程序也有类似的病毒行为，称为类病毒行为。例如：

（1）杀病毒工具去写有毒的可执行程序。

（2）某些安装程序动态修改可执行程序。

（3）加密程序对被加密程序的写入行为。

（4）反病毒工具携带某些数据文件，这些文件中的某些随机数据非常类似于反病毒工具的判据。

（5）某些程序自己修改自己，如 MS-DOS 系统的 SETVER.EXE。

病毒行为监控工具遇到上述具有类病毒行为的正常程序时就会误报警。

完全没有误报警的工具是十分理想的，然而，凡是采用病毒行为做判据的反病毒工具难以做到不误报警。误报警会对不懂计算机的用户带来惊吓和误导。只有对于计算机和病毒比较了解的人，对误报警才能具体分析。

行为监测技术的优点有：可发现未知病毒、可相当准确地预报未知的多数病毒。行为监测技术的不足是：可能误报警、不能识别病毒名称和实现时有一定难度。

6）主动防御技术

主动防御技术是指以“程序行为自主分析判定法”为理论基础，其关键是从反病毒领域普遍遵循的计算机病毒的定义出发，采用动态仿真技术，依据专家分析程序行为、判定程序性质的逻辑，模拟专家判定病毒的机理，实现对新病毒提前防御。

主动防御是一种阻止恶意程序执行的技术。它比较好地弥补了传统杀毒软件采用“特征码查杀”和“监控”相对滞后的技术弱点，可以在病毒发作时进行主动而有效的全面防范，从技术层面上有效应对未知病毒的肆虐。

主动防御技术并不是一项全新的技术，从某种程度上说，其集成了启发式扫描技术和行为监控及行为阻断等技术。

2．典型反病毒产品介绍

目前知名的反病毒软件厂商很多，部分列表如下。

杀 毒 软 件	开发公司/开发者
瑞星杀毒软件	北京瑞星科技股份有限公司
金山毒霸	金山软件公司
江民杀毒软件	北京江民新科技术有限公司
安天防线	安天实验室
微点主动防御软件	东方微点
AntiVir	AVIRA
Avast!	ALWIL Software
AVG	Grisoft
BitDefender	SoftWin SRL
Clam AntiVirus	Tomasz Kojm
Dr.Web	Dr.Web 有限公司
F-Secure	F-Secure
Kaspersky（卡巴斯基）	Kaspersky Lab
McAfee	McAfee
NOD32	Eset
Norton（诺顿）	赛门铁克
Norman Anti-Virus	Norman
Windows Defender	微软
Windows Live OneCare	微软
Panda	Panda Software
PC-cillin	趋势科技
Sophos	Sophos Plc
驱逐舰杀毒软件	New Technology Wave Incorporated

4.2 黑客攻击及其预防

4.2.1 黑客和黑客攻击

黑客（Hacker）在当前的网络世界中有褒贬两重含义。从褒义方面讲，黑客特指一些特别优秀的程序员或技术专家。1998 年，日本出版了《新黑客字典》，可以看到上面对黑客的定义是："喜欢探索软件程序奥秘、并从中增长其个人才干的人。他们不像绝大多数计算机使用者，只规规矩矩地了解别人指定了解的范围狭小的部分知识"。他们对于

操作系统和编程语言有着深刻的认识，乐于探索操作系统的奥秘且善于通过探索了解系统中的漏洞及其原因所在，他们恪守这样一条准则：Never damage any system（永不破坏任何系统）。从贬义方面讲，黑客是一些蓄意破坏计算机和电话系统的人。真正的黑客把这些人叫做“骇客（cracker）”，并不屑与之为伍。专门以破坏别人安全为目的的行为并不能使你成为一名黑客，正如用铁丝偷开走汽车并不能使你成为一个汽车工程师。

这里主要介绍一些黑客的基本知识，包括信息的收集和攻击的方式。

1．信息的收集

黑客攻击的效果和他们对目标的了解程度有着直接的相关性。因此，信息收集在攻击过程中占据着头等重要位置，包括财务数据、硬件配置、人员结构、网络架构和整体利益等诸多方面。而且因特网上的共享资源可以为几乎任何攻击阶段提供有价值的信息。信息收集的主要方式如下。

（1）网络监测。一类快速检测网络中计算机漏洞的工具。包括嗅探应用软件，能在计算机内部或通过网络来捕捉传输过程中的密码等数据信息。

（2）社会工程。运用操纵技巧来获取信息，例如，在喝啤酒交谈过程中询问对方密码或账号等信息，或是伪装成另一个人骗取信息。

（3）公共资源和垃圾。从公开的广告资料甚至是垃圾中收集信息。

（4）后门工具。这是一些工具包，用来掩盖计算机安全已受到威胁的事实。

2．黑客攻击方式

黑客主要的攻击方式有以下几种。

（1）拒绝服务攻击。

（2）缓冲区溢出攻击。

（3）漏洞攻击。

（4）欺骗攻击

4.2.2　拒绝服务攻击与防御

拒绝服务攻击（Denial of Service，DoS）是由人为或非人为发起的行动，使主机硬件、软件或者两者同时失去工作能力，使系统不可访问并因此拒绝合法的用户服务要求。拒绝服务攻击的主要企图是借助于网络系统或网络协议的缺陷和配置漏洞进行网络攻击，使网络拥塞、系统资源耗尽或者系统应用死锁，妨碍目标主机和网络系统对正常用户服务请求的及时响应，造成服务的性能受损甚至导致服务中断。

要对服务器实施拒绝服务攻击，有两种思路。

（1）服务器的缓冲区满，不接收新的请求。

（2）使用 IP 欺骗，迫使服务器把合法用户的连接复位，影响合法用户的连接。这也是 DoS 攻击实施的基本思想。

1．传统拒绝服务攻击的分类

拒绝服务攻击有许多种，网络的内外部用户都可以发动这种攻击。内部用户可以通过长时间占用系统的内存、CPU 处理时间使其他用户不能及时得到这些资源，而引起拒绝服务攻击；外部黑客也可以通过占用网络连接使其他用户得不到网络服务。本节主要讨论外部用户实施的拒绝服务攻击。

外部用户针对网络连接发动拒绝服务攻击主要有以下几种模式。

（1）消耗资源。计算机和网络需要一定的条件才能运行，如网络带宽、内存、磁盘空间和 CPU 时间。攻击者利用系统资源有限这一特征，或者是大量地申请系统资源，并长时间地占用；或者是不断地向服务程序发请求，使系统忙于处理自己的请求，而无暇为其他用户提供服务。攻击者可以针对以下几种资源发起拒绝服务攻击。

① 针对网络连接的拒绝服务攻击。

② 消耗磁盘空间。

③ 消耗 CPU 资源和内存资源。

（2）破坏或更改配置信息。计算机系统配置上的错误也可能造成拒绝服务攻击，尤其是服务程序的配置文件以及系统、用户的启动文件。这些文件一般只有该文件的属主才可以写入，如果权限设置有误，攻击者（包括已获得一般访问权的黑客与恶意的内部用户）可以修改配置文件，从而改变系统向外提供服务的方式。

（3）物理破坏或改变网络部件。这种拒绝服务针对的是物理安全，一般来说，通过物理破坏或改变网络部件以达到拒绝服务的目的。其攻击的目标有计算机、路由器、网络配线室、网络主干段、电源、冷却设备和其他的网络关键设备。

（4）利用服务程序中的处理错误使服务失效。最近出现了一些专门针对 Windows 系统的攻击方法，如 LAND 等。被这些工具攻击之后，目标机的网络连接就会莫名其妙地断掉，不能访问任何网络资源，或者出现莫名其妙的蓝屏，系统进入死锁状况。这些攻击方法主要利用服务程序中的处理错误，发送一些该程序不能正确处理的数据包，引起该服务进入死循环。

2．分布式拒绝服务攻击

分布式拒绝服务（Distributed Denial of Service，DDoS）攻击是对传统 DoS 攻击的发展，攻击者首先侵入并控制一些计算机，然后控制这些计算机同时向一个特定的目标发起拒绝服务攻击。传统的拒绝服务攻击有受网络资源的限制和隐蔽性差两大缺点，而分布式拒绝服务攻击克服了传统拒绝服务攻击的这两个致命弱点。分布式拒绝服务攻击的隐蔽性更强。通过间接操纵网络上的计算机实施攻击，突破了传统攻击方式从本地攻击的局限性。被 DDoS 攻击时可能的现象如下。

（1）被攻击主机上有大量等待的 TCP 连接。

（2）大量到达的数据分组（包括 TCP 分组和 UDP 分组）并不是网站服务连接的一部分，往往指向机器的任意端口。

（3）网络中充斥着大量的无用数据包，源地址为假。

（4）制造高流量的无用数据，造成网络拥塞，使受害主机无法正常和外界通信。

（5）利用受害主机提供的服务和传输协议上的缺陷，反复发出服务请求，使受害主机无法及时处理所有正常请求。

（6）严重时会造成死机。

DDoS 引入了分布式攻击和 Client/Server 结构，使 DoS 的威力激增。同时，DDoS 囊括了已经出现的各种重要的 DoS 攻击方法，比 DoS 的危害性更大。现有的 DDoS 工具一般采用三级结构，如图 4-4 所示。其中，Client（客户端）运行在攻击者的主机上，用来发起和控制 DDoS 攻击；Handler（主控端）运行在已被攻击者侵入并获得控制的主机上，用来控制代理端；Agent（代理端）运行在已被攻击者侵入并获得控制的主机上，从主控端接收命令，负责对目标实施实际的攻击。

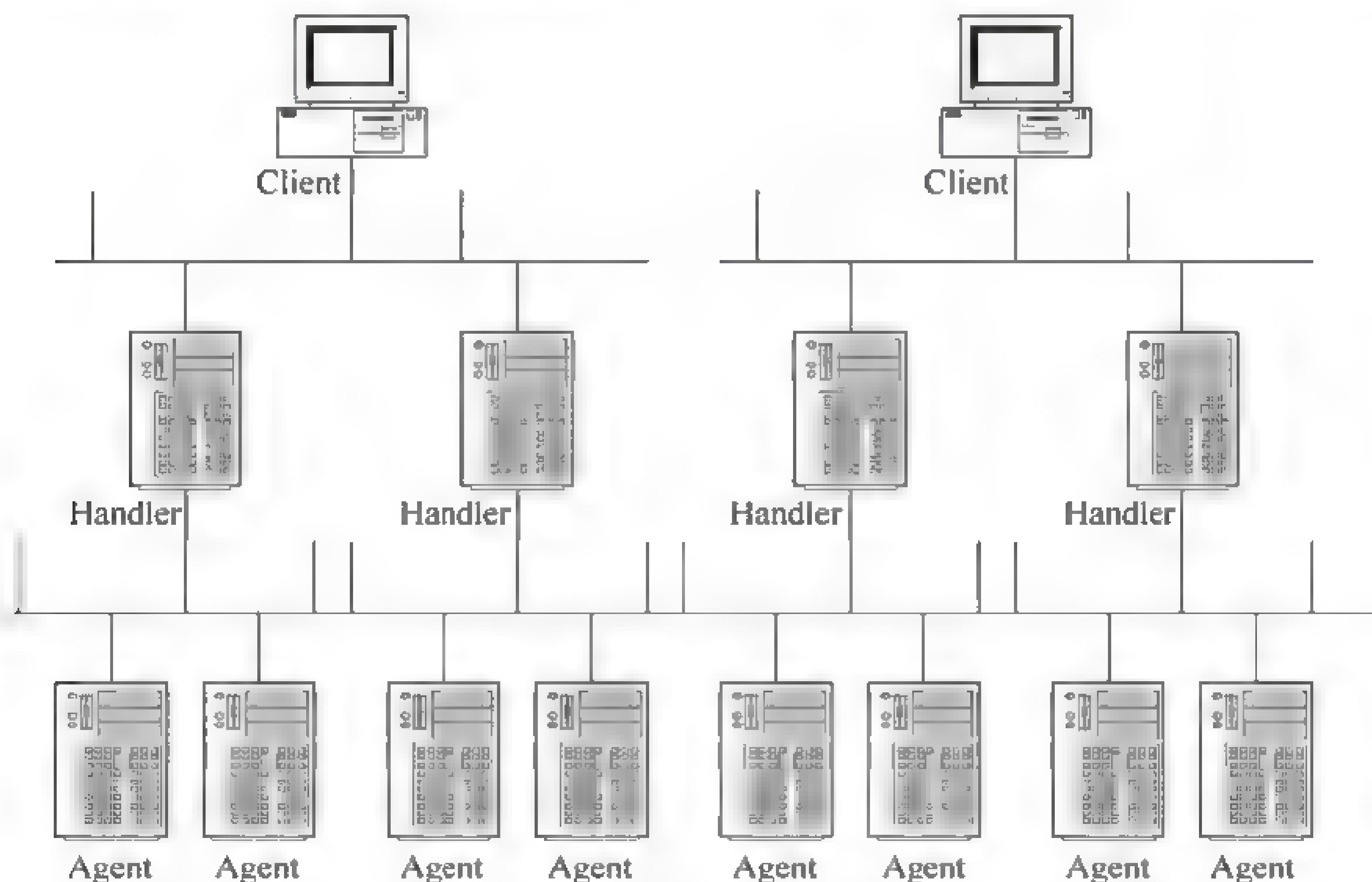


图 4-4　DDoS 的三级控制结构

3．拒绝服务攻击的防御方法

操作系统和网络设备的缺陷在不断地被发现并被攻击者所利用来进行恶意的攻击。如果清楚地认识到这一点，应当使用下面的方法尽量阻止拒绝服务攻击。

（1）加强对数据包的特征识别，攻击者在传达攻击命令或发送攻击数据时，虽然都加入了伪装甚至加密，但是其数据包中还是有一些特征字符串。通过搜寻这些特征字符串，就可以确定攻击服务器和攻击者的位置。

（2）设置防火墙监视本地主机端口的使用情况。对本地主机中的敏感端口，如 UDP 31335、UDP 27444、TCP 27665，进行监视，如果发现这些端口处于监听状态，则系统

很可能受到攻击。即使攻击者已经对端口的位置进行了一定的修改，但如果外部主机主动向网络内部高标号端口发起连接请求，则系统也很可能受到侵入。

（3）对通信数据量进行统计也可获得有关攻击系统的位置和数量信息。例如，在攻击之前，目标网络的域名服务器往往会接收到远远超过正常数量的反向和正向的地址查询。在攻击时，攻击数据的来源地址会发出超出正常极限的数据量。

（4）尽可能地修正已经发现的问题和系统漏洞。

4.2.3 缓冲区溢出攻击与防御

缓冲区溢出攻击是一种通过往程序的缓冲区写超出其长度的内容，造成缓冲区溢出，从而破坏程序的堆栈，使程序转而执行其他预设指令，以达到攻击目的的攻击方法。缓冲区溢出是一个非常普遍、非常严重的漏洞，在各种操作系统中广泛存在。

1. 缓冲区溢出攻击原理

缓冲区是计算机内存中的一个连续块，保存了给定类型的数据。当进行大量动态内存分配而又管理不当时，就会出现问题。动态变量所需要的缓冲区，是在程序运行时才进行分配的。如果程序在动态分配的缓冲区中放入超长的数据，它就会溢出。缓冲区溢出攻击的基本原理是向缓冲区中写入超长的、预设的内容，导致缓冲区溢出，覆盖其他正常的程序或数据，然后让计算机转去运行这行预设的程序，达到执行非法操作、实现攻击的目的。

2. 缓冲区溢出实例

众所周知，C 语言不进行数组的边界检查。在许多 C 语言实现的应用程序中，都假定缓冲区的长度是足够的，即它的长度肯定大于要复制的字符串的长度，事实上却并非如此。通常，一个程序在内存中分为程序段、数据段和堆栈三部分。程序段里放着程序的机器码和只读数据；数据段放程序中的静态数据；动态数据则通过堆栈来存放。在内存中，它们的位置如图 4-5 所示。



图 4-5 一个程序在内存中的存放

举一个简单的例子描述上述过程：

```
void main()
{
  int t;
  char buffer[128];
  for (i=0;i<127;i++)
   buffer[i] ='A';
  buffer[127]=0;
  function (buffer) ;
```

```
void function (char *str)
    {
       char buffer[16];
       strcpy (buffer, str) ;
}
```

```
    print ("This is a test\n");
}
```

这是一个典型的存在缓冲区溢出错误的程序。在函数 function()中，将一个 128 字节长度的字符串复制到只有 16 字节长的局部缓冲区中，在调用 strcpy()进行字符串复制时没有进行缓冲区越界检查。在图 4-6 中可以看到执行函数 function()时的堆栈情形。



图 4-6　调用函数 function()时堆栈的情形

执行此程序得不到输出 This is a test。因为程序没有执行到这一步，当程序执行到 function()时，子程序执行完毕，应返回到执行 print（"This is a test\n"）处。但是，由于缓冲区已经溢出，子程序的返回地址变成了 0x41414141——一个显然还在进程地址空间但已不是程序正常流程的地址，无法预料在这里程序会执行什么指令，但本程序很小，不会引起严重后果。因为 0x41414141 是在主程序中对字符串数组赋值时写入的值，可以设想，假如在主程序中对字符串数组赋值时，将一个有危险指令序列的地址以字符串方式填入在刚好覆盖子程序返回地址的数组位置，那么子程序执行完返回时，就会执行这一段危险指令，其后果将是不可预料的。

3. 缓冲区溢出程序的要素及执行步骤

通过上面的分析可知，修改程序的返回地址，让它去执行一段精心准备的程序，可以达到攻击的目的。一个缓冲区溢出程序的执行通常由以下 4 个步骤组成。

（1）准备一段可以调出一个 shell 的机器码形式的字符串，称之为 SHELLCODE。

（2）申请一个缓冲区，并将机器码填入缓冲区的低端。

（3）估算机器码在堆栈中的起始位置，并将这个位置写入缓冲区的高端。

（4）将这个缓冲区作为系统的一个有着缓冲区溢出错误的程序的入口参数，并执行这个有错误的程序。

总而言之，这种攻击能够成功主要是利用了程序中边界条件、函数指针等设计不当的漏洞，即利用了 C 程序本身的不安全性。而大多数 UNIX、Linux、Windows 系统的开发都依赖于 C 语言，所以缓冲区溢出攻击成为操作系统、数据库等应用程序最普遍的漏洞之一。

4．缓冲区溢出攻击的防御

缓冲区溢出攻击的防范是和整个系统的安全性分不开的。如果整个网络系统的安全设计很差，则遭受缓冲区溢出攻击的机会也大大增加。针对缓冲区溢出，可以采取多种防范策略。

1）系统管理上的防范策略

（1）关闭不需要的特权程序。

（2）及时给程序漏洞打补丁。

2）软件开发过程中的防范策略

发生缓冲区溢出的主要及各要素是：数组没有边界检查而导致的缓冲区溢出；函数返回地址或函数指针被改变，使程序流程的改变成为可能；植入代码被成功地执行等。所以针对这些要素，从技术上可以采取一定的措施。

（1）编写正确的代码。只要在所有复制数据的地方进行数据长度和有效性的检查，确保目标缓冲区中数据不越界并有效，就可以避免缓冲区溢出，更不可能使程序跳转到恶意代码上。

（2）缓冲区不可执行。通过使被攻击程序的数据段地址空间不可执行，从而使得攻击者不可能执行被植入被攻击程序输入缓冲区的代码，这种技术被称为缓冲区不可执行技术。

（3）改进 C 语言函数库。C 语言中存在缓冲区溢出攻击隐患的系统函数有很多，如 gets()、sprintf()、strcpy()、strcat()、fscanf()、scanf()和 vsprintf()等。可以开发出更安全的封装了若干已知易受堆栈溢出攻击的库函数。

（4）使堆栈向高地址方向增长。使用的机器堆栈压入数据时向高地址方向前进，那么无论缓冲区如何溢出，都不可能覆盖低地址处的函数返回地址指针，也就避免了缓冲区溢出攻击。但是，这种方法仍然无法防范利用堆和静态数据段的缓冲区进行溢出的攻击。

（5）程序指针完整性检查。原理是每次在程序指针被引用之前先检测该指针是否已被恶意改动过，如果发现被改动，程序就拒绝执行。

（6）利用编译器将静态数据段中的函数地址指针存放地址和其他数据的存放地址分离。

4.2.4 程序漏洞攻击与防御

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。从某种意义上来说，程序存在的错误几乎在所难免。软件开发者任何一个小小的疏忽和谬误都会给入侵者以可乘之机，因此，利用处理程序的错误对系统进行攻击是黑客们惯用的手段之一。本节主要从 Web 程序和 TCP/IP 漏洞角度来探讨程序漏洞及防御。

1．Web 程序漏洞攻击与防御

1）CGI 漏洞攻击

CGI 即公共网关接口，在 Web 服务器上定义了 Web 客户请求与应答的一种方式，是外部扩展应用程序（如 perl 脚本）与 WWW 服务器交互的一个标准接口。

在计算机领域，尤其在 Internet 上，尽管大部分 Web 服务器所编的程序都尽可能保护自己的内容不受侵害，但只要 CGI 脚本中有一点安全方面的失误，如口令文件、私有数据以及任何其他敏感内容，就能使入侵者方便地侵入到计算机。遵循一些简单的规则并保持警惕能使 CGI 脚本免受侵害，从而保护用户的权益。

下面就来详细介绍一下关于 CGI 的漏洞。

（1）配置错误。主要是指 CGI 程序和数据文件的权限设置不当，导致 CGI 源代码或敏感信息泄露。还有一个经常犯的错误就是安装完 CGI 程序后没有删除安装脚本，这样攻击者就可能远程重置数据。

（2）边界条件错误。主要针对 C 语言编写的 CGI，利用这个错误，攻击者可能发起缓冲区溢出攻击，从而提升权限。

（3）访问验证错误。主要是因为用于验证的条件不足以确定用户的身份而造成的，经常会导致未经授权访问，修改甚至删除没有访问权限的内容。用于确定用户身份的方法一般有两种，一是账号和密码，二是 Session 认证。而不安全的认证方法包括 Userid 认证、Cookie 认证等等。

（4）来源验证错误。比较常见的利用这种错误进行攻击的方法就是 DoS，也就是拒绝服务攻击。如灌水机，就是利用 CGI 程序没有对文章的来源进行验证，从而不间断地发文章，最后导致服务器硬盘充满而挂起。

（5）输入验证错误。这种错误导致的安全问题最多，主要是因为没有过滤特殊字符。例如，没有过滤%20 造成的畸形注册，没有过滤“../”经常造成泄露系统文件，没有过滤“$”经常导致泄露网页中的敏感信息，没有过滤“;”经常导致执行任意系统指令，没有过滤“|”或“\t”经常导致文本文件攻击，没有过滤“’”和“#”经常导致 SQL 数据库攻击，没有过滤“<”和“>”导致的 Cross-Site Scripting 攻击等。

（6）异常情况处理失败。如没有检查文件是否存在就直接打开设备文件导致拒绝服务，没有检查文件是否存在就打开文件提取内容进行比较而绕过验证，上下文攻击导致执行任意代码等。

（7）策略错误。这种错误主要是由于编制 CGI 程序的程序员的决策造成的。如原始密码生成机制脆弱导致穷举密码，在 Cookie 中明文存放账号密码导致敏感信息泄露，使用与 CGI 程序不同的扩展名存储敏感信息导致该文件被直接下载，丢失密码模块在确认用户身份之后直接让用户修改密码而不是把密码发到用户的注册信箱，登录时采用账号和加密后的密码进行认证导致攻击者不需要知道用户的原始密码就能够登录等。

防范 CGI 脚本漏洞的主要方法如下。

（1）使用最新版本的 Web 服务器，安装最新的补丁程序，正确配置服务器。

（2）按照帮助文件正确安装 CGI 程序，删除不必要的安装文件和临时文件。

（3）使用 C 编写 CGI 程序时，使用安全的函数。

（4）使用安全有效的验证用户身份的方法。

（5）验证用户的来源，防止用户短时间内过多动作。

（6）推荐过滤"& ; ` " \ " | * ? ~ < > ^ （ ） [ ] { } $ \n \r \t \0 # ../。

（7）在设计 CGI 脚本时，其对输入数据的长度有严格限制。

（8）实现功能时制定安全合理的策略，CGI 程序还应具有检查异常情况的功能，在检查出陌生数据后 CGI 应能及时处理这些情况。

2）SQL 注入攻击

随着 BPS 模式应用开发的发展，使用这种模式编写应用程序的程序员也越来越多。但是由于程序员的水平及经验也参差不齐，相当大一部分程序员在编写代码的时候，没有对用户输入数据的合法性进行判断，使应用程序存在安全隐患。用户可以提交一段数据库查询代码，根据程序返回的结果获得某些他想得知的数据，这就是所谓的 SQL Injection，即 SQL 注入。SQL 注入是从正常的 WWW 端口访问，而且表面看起来跟一般的 Web 页面访问没什么区别，所以目前市面的防火墙都不会对 SQL 注入发出警报，如果管理员没查看 IIS 日志的习惯，可能被入侵很长时间都不会发觉。但是，SQL 注入的手法相当灵活，在注入的时候会碰到很多意外的情况。需要根据具体情况进行分析，构造巧妙的 SQL 语句，从而成功获取想要的数据。

SQL 注入攻击的过程主要包含以下几步。

（1）发现 SQL 注入位置。

（2）判断后台数据库类型。

（3）确定 XP_CMDSHELL 可执行情况。

（4）发现 Web 虚拟目录。

（5）上传 ASP 木马。

（6）得到管理员权限。

针对 SQL 注入攻击，可以使用下面的方法进行防御。

（1）下载 SQL 通用防注入系统的程序，在需要防范注入的页面头部用<!--# include file="xxx.asp"-->来防止攻击者进行手动注入测试。可是攻击者通过 SQL 注入分析器就可轻松跳过防注入系统并自动分析其注入点，然后只需几秒钟，管理员账号及密码就会被分析出来。

（2）对于注入分析器的防范，首先要知道 SQL 注入分析器是如何工作的。如果分析器并不是针对 admin 管理员账号，而是针对权限（如 flag=1），那么无论管理员账号怎么变都无法逃过检测。

（3）既然无法逃过检测，那可以建立两个账号，一个是普通的管理员账号，一个是防注入的账号。利用一个权限最大的账号制造假象，吸引软件的检测，而这个账号里的内容是大于千字以上的中文字符，就会迫使软件对这个账号进行分析的时候进入全负荷状态甚至资源耗尽而死机。

下面进行数据库的修改。

① 对表结构进行修改。将防注入账号字段的数据类型进行修改，文本型改成最大字段 255，密码的字段也进行相同的设置。

② 对表进行修改。设置防注入账号在 ID1，并输入大量中文字符。

③ 把真正的管理员密码放在 ID2 后的任何一个位置。

完成三步对数据库的修改后，还需要限制向管理员登录的页面文件中写入字符，如此即使攻击者破解密码也无法登录，而真正的密码则可以不受限制。

2．TCP/IP 漏洞

这种攻击主要是利用 TCP/IP 协议实现中的处理程序错误实施拒绝服务攻击，即故意错误地设定数据包头的一些重要字段（如 IP 包头部的 Total Length、Fragment offset、IHL 和 Source address 等），使用 Raw Socket 将这些错误的 IP 数据包发送出去。在接收数据端，服务程序通常都存在一些问题，因而在将接收到的数据包组装成一个完整的数据包的过程中，就会引起系统死机、挂起或崩溃，无法继续提供服务。这些攻击包括 Ping of Death 攻击、Teardrop 攻击、Winnuke 攻击以及 Land 攻击等。

1）Ping of Death 攻击

根据 TCP/IP 协议的规范，一个包的长度最大为 65 536 字节。尽管一个包的长度最大不能超过 65 536 字节，但是一个包分成的多个片段的叠加却能做到。当一个主机收到了长度大于 65 536 字节的包时，就是受到了 Ping of Death 攻击，该攻击会造成主机死机。攻击者故意创建一个长度大于 65 536 字节（IP 协议中规定最大的 IP 包长为 65 536 字节）的 ping 包，并将该包发送到目标受害主机，由于目标主机的服务程序无法处理过大的包，而引起系统崩溃、挂起或重启。

由于在早期阶段，路由器对所传输的数据包的最大尺寸都有限制，许多操作系统对 TCP/IP 的实现在 ICMP 包上都是规定 64KB，并且在对包的标题头进行读取之后，要根

据该标题头里包含的信息来为有效载荷生成缓冲区，一旦产生畸形即声明自己的尺寸超过 ICMP 上限的包，也就是加载的尺寸超过 64KB 上限时，就会出现内存分配错误，导致 TCP/IP 堆栈崩溃，致使接收方死机。这种攻击方式主要是针对 Windows 操作系统，而 UNIX、Linux、Solaris、Mac OS 都具有抵抗一般 Ping of Death 攻击的能力。目前，所有的操作系统都对此进行了修补或升级。

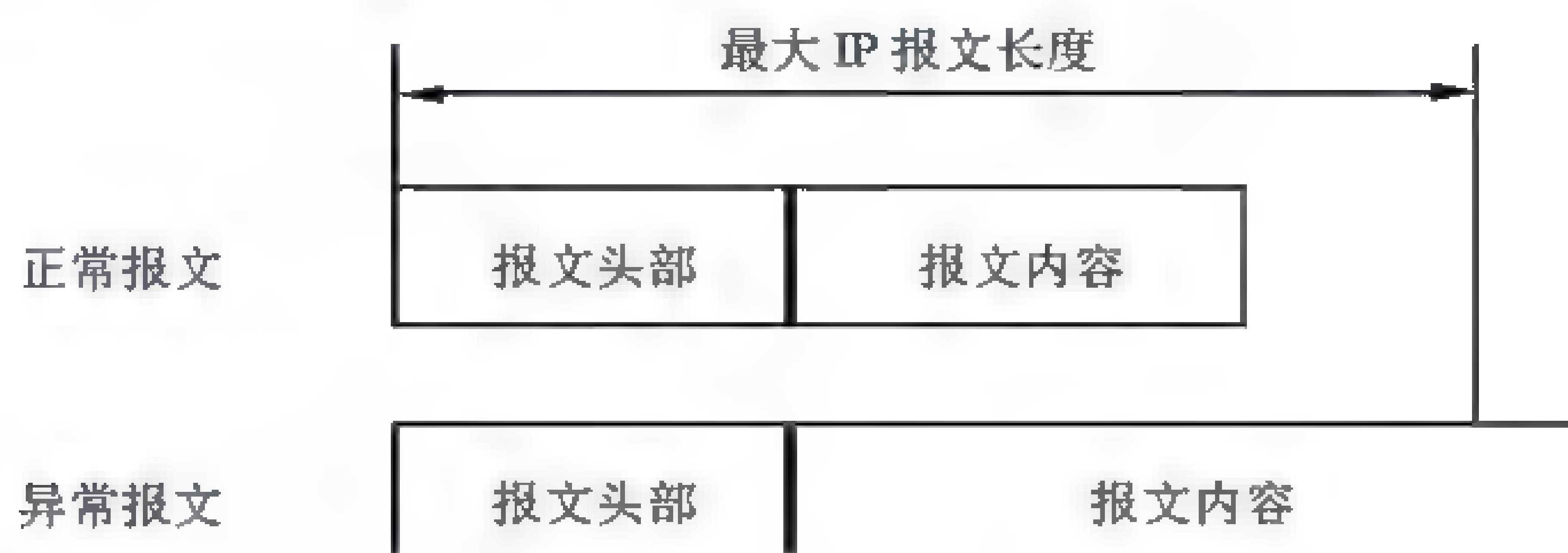


图 4-7 Ping of Death 攻击报文

2）Teardrop 攻击

一个 IP 分组在网络中传播时，由于沿途各个链路的最大传输单元不同，路由器常常会对 IP 包进行分组，即将一个包分成一些片段，使每段都足够小，以便通过这个狭窄的链路。每个片段将具有完整的 IP 包头，其大部分内容和最初的包头相同，一个很典型的不同在于包头中还包含偏移量（offset）字段。随后各片段将沿着各自的路径独立地转发到目的地，在目的地最终将各片段进行重组。这就是所谓的 IP 包的分段/重组技术。

Teardrop 攻击就是利用 IP 包的分段/重组技术在系统实现中的一个错误，即在组装 IP 包时只检查了每段数据是否过长，而没有检查包中有效数据的长度是否过小。当包中数据长度为负时，由于 memcpy()中的计数器是一个反码，负数表示一个非常大的数值。因为 IP 包重组和缓冲区通常处于系统核心态，缓冲区溢出将使系统崩溃。攻击者可以通过发送两段（或者更多）数据包来实现 Teardrop 攻击。实现攻击的数据包中，第一个包的偏移量为 0，长度为 N，第二个包的偏移量小于 N。为了合并这些数据段，TCP/IP 堆栈会分配超乎寻常的巨大资源，从而造成系统资源的缺乏，甚至机器重新启动。

3）Winnuke 攻击

Winnuke 攻击针对 Windows 系统上一般都开放的 139 端口，这个端口由 NetBIOS 使用。只要往该端口发送 1 字节 TCP OOB 数据，就可以使 Windows 系统出现“蓝屏”错误，并且网络功能完全瘫痪。除非重新启动，否则不能再用。

带外数据（Out of Band，OOB）是指 TCP 连接中发送的一种特殊数据，它的优先级高于一般的数据。带外数据在报头中设置了 URG 标志，可以不按照通常的次序进入 TCP 缓冲区，而是进入另外一个缓冲区，可立即被进程读取；或者可以根据进程的设置，直接用 SIGURG 信号通知进程有带外数据到来。

4）Land 攻击

Land 也是一个十分有效的攻击工具，它对当前流行的大部分操作系统及一部分路由器都具有相当的攻击能力。攻击者利用目标受害系统的自身资源实现攻击意图。由于目标受害系统具有漏洞和通信协议的弱点，这样就给攻击者提供了攻击的机会。攻击者将一个包的源地址和目的地址都设置为目标主机的地址，然后将该包通过 IP 欺骗的方式发送给被攻击主机，这种包可以造成被攻击主机因试图与自己建立连接而陷入死循环，从而很大程度地降低了系统性能。

在 Land 攻击中，SYN 包中的源地址和目标地址都被设置成某一个服务器地址，这时将导致接受服务器向它自己的地址发送 SYN＋ACK 消息，结果这个地址又发回 ACK 消息并创建一个空连接，每一个这样的连接都将保留直到超时。对 Land 攻击反应不同，许多 UNIX 实现将崩溃，而 Windows 会变得极其缓慢。

对于这些利用 TCP/IP 协议实现中的处理程序错误实施的攻击，最有效最直接的防御方法是尽早发现潜在的错误并及时修正。从长远角度考虑，在编制软件的时候应更多地考虑安全问题，提高代码质量，减少安全漏洞。

4.2.5　欺骗攻击与防御

1．ARP 欺骗

1）ARP 欺骗原理

ARP 原理：某机器 A 要向主机 C 发送报文，会查询本地的 ARP 缓存表，找到 C 的 IP 地址对应的 MAC 地址后，就会进行数据传输。如果未找到，则广播一个 ARP 请求报文（携带主机 A 的 IP 地址 Ia——物理地址 AA:AA:AA:AA），请求 IP 地址为 Ic 的主机 C 回答物理地址 Pc。网上所有主机包括 C 都收到 ARP 请求，但只有主机 C 识别自己的 IP 地址，于是向 A 主机发回一个 ARP 响应报文。其中就包含有 C 的 MAC 地址 CC:CC:CC:CC，A 接收到 C 的应答后，就会更新本地的 ARP 缓存。接着使用这个 MAC 地址发送数据（由网卡附加 MAC 地址）。因此，本地高速缓存的这个 ARP 表是本地网络流通的基础，而且这个缓存是动态的。

ARP 协议并不只在发送了 ARP 请求才接收 ARP 应答。当计算机接收到 ARP 应答数据包的时候，就会对本地的 ARP 缓存进行更新，将应答中的 IP 和 MAC 地址存储在 ARP 缓存中。因此，局域网中的机器 B 首先攻击 C 使 C 瘫痪，然后向 A 发送一个自己伪造的 ARP 应答，而如果这个应答是 B 冒充 C 伪造来的，即 IP 地址为 C 的 IP，而 MAC 地址是 B 的，则当 A 接收到 B 伪造的 ARP 应答后，就会更新本地的 ARP 缓存，这样在 A 看来 C 的 IP 地址没有变，而它的 MAC 地址已经变成 B 的了。由于局域网的网络流通不是根据 IP 地址进行，而是按照 MAC 地址进行传输。如此就造成 A 传送给 C 的数据实际上是传送到 B。这就是一个简单的 ARP 欺骗，如图 4-8 所示。

2）ARP 欺骗的防范措施

（1）在 winxp 下输入命令 arp-s gate-way-ip gate-way-mac 固化 arp 表，阻止 arp 欺骗。

（2）使用 ARP 服务器。通过该服务器查找自己的 ARP 转换表来响应其他机器的 ARP 广播。确保这台 ARP 服务器不被黑。

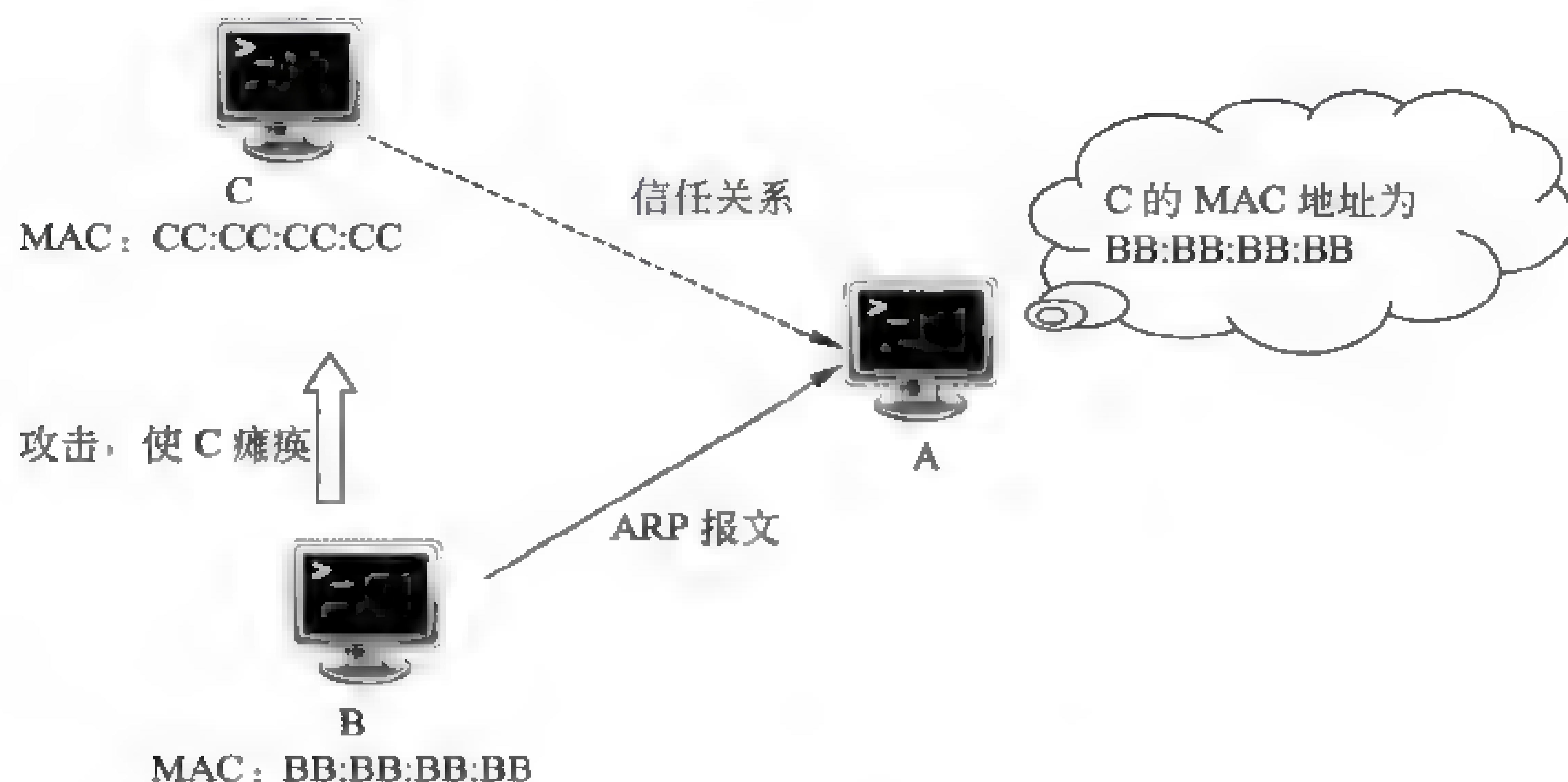


图 4-8　ARP 欺骗

（3）采用双向绑定的方法解决并且防止 ARP 欺骗。

（4）ARP 防护软件——ARP Guard。通过系统底层核心驱动，无需安装其他任何第三方软件（如 WinPcap），以服务及进程并存的形式随系统启动并运行，不占用计算机系统资源。无需对计算机进行 IP 地址及 MAC 地址绑定，从而避免了大量且无效的工作量。也不用担心计算机会在重启后新建 ARP 缓存列表，因为此软件是以服务与进程相结合的形式存在于计算机中，当计算机重启后软件的防护功能也会随操作系统自动启动并工作。

2．DNS 欺骗

DNS 欺骗是一种比较常见的攻击手段。一个著名的利用 DNS 欺骗进行攻击的案例，是全球著名网络安全销售商 RSA Security 的网站所遭到的攻击。其实 RSA Security 网站的主机并没有被入侵，而是 RSA 的域名被黑客劫持，当用户连上 RSA Security 时，发现主页被改成了其他的内容。

1）DNS 欺骗的原理

DNS 欺骗首先是冒充域名服务器，然后把查询的 IP 地址设为攻击者的 IP 地址，这样，用户上网就只能看到攻击者的主页，而不是用户想要取得的网站的主页了，这就是 DNS 欺骗的基本原理。DNS 欺骗其实并不是真的“黑掉”了对方的网站，而是冒名顶替、招摇撞骗罢了。

2）DNS 欺骗的实现过程

如图 4-9 所示，www.xxx.com的 IP 地址为 202.109.2.2，如果 www.angel.com 向 xxx.com 的子域 DNS 服务器查询www.xxx.com的 IP 地址时，www.heike.com 冒充 DNS 向 www.angel.com 回复www.xxx.com的 IP 地址为 200.1.1.1，这时 www.angel.com 就会把

200.1.1.1 当www.xxx.com的地址了。当 www.angel.com 连www.xxx.com时，就会转向那个虚假的 IP 地址了，这样对www.xxx.com来说，就算是给黑掉了。因为别人根本连接不上他的域名。

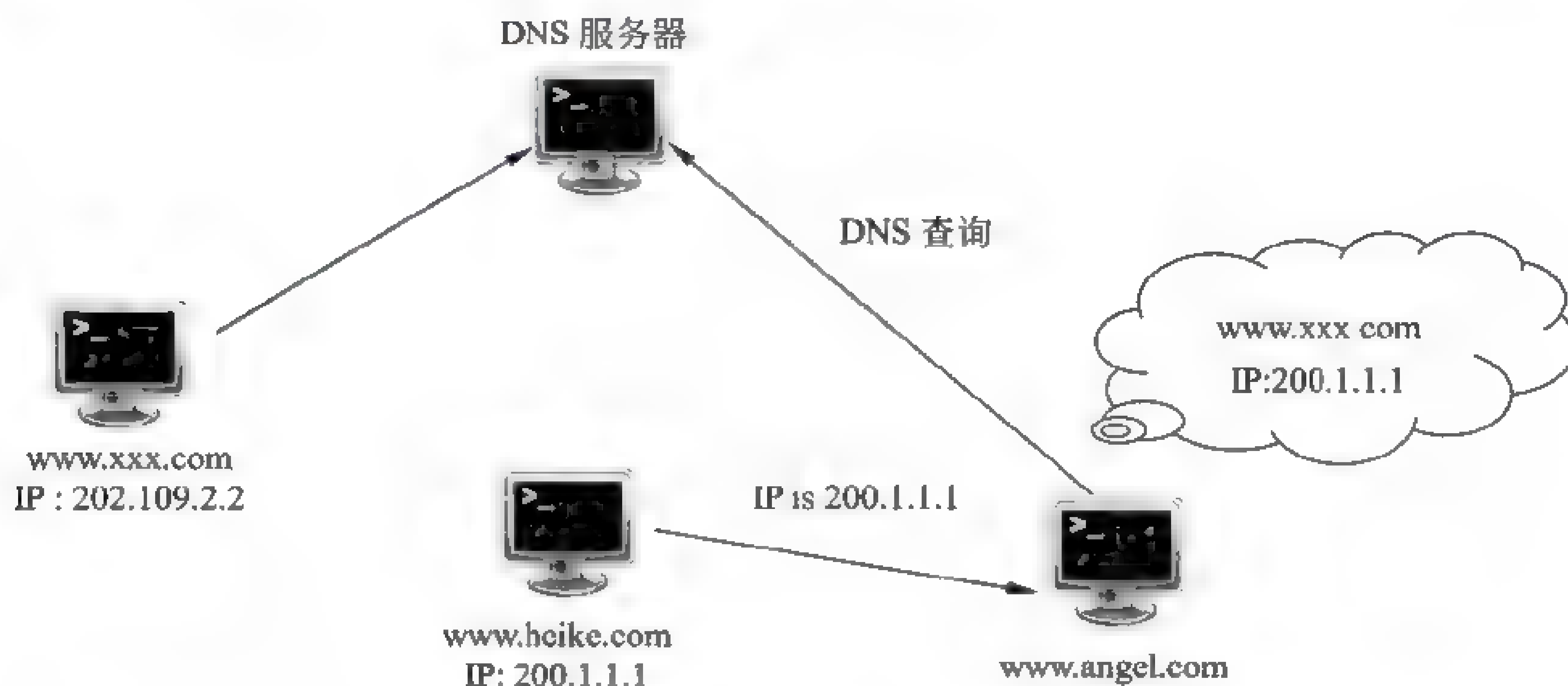


图 4-9　DNS 欺骗

3）DNS 欺骗的检测

根据检测手段的不同，将其分为被动监听检测、虚假报文探测和交叉检查查询三种。

（1）被动监听检测。该检测手段是通过旁路监听的方式，捕获所有 DNS 请求和应答数据包，并为其建立一个请求应答映射表。如果在一定的时间间隔内，一个请求对应两个或两个以上结果不同的应答包，则怀疑受到了 DNS 欺骗攻击，因为 DNS 服务器不会给出多个结果不同的应答包，即使目标域名对应多个 IP 地址，DNS 服务器也会在一个 DNS 应答包中返回，只是有多个应答域（answer section）而已。

（2）虚假报文探测。该检测手段采用主动发送探测包的手段来检测网络内是否存在 DNS 欺骗攻击者。这种探测手段基于一个简单的假设：攻击者为了尽快地发出欺骗包，不会对域名服务器 IP 的有效性进行验证。这样，如果向一个非 DNS 服务器发送请求包，正常来说不会收到任何应答，但是由于攻击者不会验证目标 IP 是否是合法 DNS 服务器，它会继续实施欺骗攻击，因此如果收到了应答包，则说明受到了攻击。

（3）交叉检查查询。所谓交叉检查，即在客户端收到 DNS 应答包之后，向 DNS 服务器反向查询应答包中返回的 IP 地址所对应的 DNS 名字，如果二者一致说明没有受到攻击，否则说明被欺骗。

3．IP 欺骗

1）IP 欺骗的原理

通过编程的方法可以随意改变发出的包的 IP 地址，但工作在传输层的 TCP 协议是一种相对可靠的协议，不会让黑客轻易得逞。由于 TCP 是面向连接的协议，所以在双方

正式传输数据之前，需要用“三次握手”来建立一个值得信赖的连接。假设是 hosta 和 hostb 两台主机进行通信，hostb 首先发送带有 SYN 标志的数据段通知 hosta 建立 TCP 连接，TCP 的可靠性就是由数据包中的多位控制字来提供的，其中最重要的是数据序列 SYN 和数据确认标志 ACK。B 将 TCP 报头中的 SYN 设为自己本次连接中的初始值（ISN）。

假如想冒充 hostb 对 hosta 进行攻击，就要先使用 hostb 的 IP 地址发送 SYN 标志给 hosta，但是当 hosta 收到后，并不会把 SYN+ACK 发送到欺骗者的主机上，而是发送到真正的 hostb 上去，这时就“露陷”了，因为 hostb 根本没发送 SYN 请求。所以如果要冒充 hostb，首先要让 hostb 失去工作能力。也就是所谓的拒绝服务攻击，让 hostb 瘫痪。

可是这样还是远远不够的，最困难的就是要对 hosta 进行攻击，必须知道 hosta 使用的 ISN。TCP 使用的 ISN 是一个 32 位的计数器，从 0 到 4 294 967 295。TCP 为每一个连接选择一个初始序列号 ISN，为了防止因为延迟、重传等扰乱三次握手，ISN 不能随便选取，不同的系统有着不同的算法。ISN 约每秒增加 128 000，如果有连接出现，每次连接将把计数器的数值增加 64 000。很显然，这使得用于表示 ISN 的 32 位计数器在没有连接的情况下每 9.32 小时复位一次。之所以这样，是因为它有利于最大于限度地减少“旧有”连接的信息干扰当前连接的机会。如果初始序例号是随意选择的，那么不能保证现有序例号是不同于先前的。假设有这样一种情况，在一个路由回路中的数据包最终跳出循环，回到了“旧有”的连接，显然这会对现有连接产生干扰。

预测出攻击目标的序列号非常困难，而且各个系统也不相同，在 Berkeley 系统，最初的序列号变量由一个常数每秒加 1 产生，等加到这个常数的一半时，就开始一次连接。这样，如果开始一个合法连接，并观察到一个 ISN 正在使用，便可以进行预测，而且这样做有很高的可信度。现在假设黑客已经使用某种方法，能预测出 ISN。在这种情况下，他就可以将 ACK 序号送给 hosta，这时连接就建立了。

2）IP 欺骗的防范

虽然 IP 欺骗攻击有着相当难度，但这种攻击非常广泛，入侵往往由这里开始。预防这种攻击可以删除 UNIX 中所有的/etc/hosts.equiv、$HOME/.rhosts 文件，修改/etc/inetd.conf 文件，使得 RPC 机制无法应用。另外，还可以通过设置防火墙过滤来自外部而信源地址却是内部 IP 的报文。

4.2.6 端口扫描

网络中的每一台计算机如同一座城堡，在这些城堡中，有的对外完全开放，有的却是紧锁城门。在网络技术中，把这些城堡的城门称之为计算机的“端口”。端口扫描是入侵者搜集信息的几种常用手法之一，也正是这一过程最容易使入侵者暴露自己的身份和意图。一般来说，扫描端口有如下目的。

（1）判断目标主机上开放了哪些服务。

（2）判断目标主机的操作系统。

如果入侵者掌握了目标主机开放了哪些服务，运行何种操作系统，他们就能够使用相应的手段实现入侵。

1．端口扫描原理

“端口”在计算机网络领域中是个非常重要的概念。它是专门为计算机通信而设计的，不是硬件，不同于计算机中的“插槽”，可以说是个“软插槽”。如果有需要，一台计算机中可以有上万个端口。

端口是由计算机的通信协议 TCP/IP 协议定义的。其中规定，用 IP 地址和端口作为套接字，它代表 TCP 连接的一个连接端，一般称为 Socket。具体来说，就是用[IP：端口]来定位一台主机中的进程。可以做这样的比喻，端口相当于两台计算机进程间的大门，可以随便定义，其目的只是为了让两台计算机能够找到对方的进程。计算机就像一座大楼，这个大楼有好多入口（端口），进到不同的入口中就可以找到不同的公司（进程）。如果要和远程主机 A 的程序通信，那么只要把数据发向[A：端口]就可以实现通信了。

端口扫描就是尝试与目标主机的某些端口建立连接，如果目标主机该端口有回复（见三次握手中的第二次），则说明该端口开放，即为“活动端口”。

2．扫描原理分类

（1）全 TCP 连接。这种扫描方法使用三次握手，与目标计算机建立标准的 TCP 连接。需要说明的是，这种古老的扫描方法很容易被目标主机记录。

（2）半打开式扫描（SYN 扫描）。在这种扫描技术中，扫描主机自动向目标计算机的指定端口发送 SYN 数据段，表示发送建立连接请求。

① 如果目标计算机的回应 TCP 报文中 SYN=1，ACK=1，则说明该端口是活动的，接着扫描主机传送一个 RST 给目标主机拒绝建立 TCP 连接，从而导致三次握手过程的失败。

② 如果目标计算机的回应是 RST，则表示该端口为“死端口”，这种情况下，扫描主机不用做任何回应。

由于扫描过程中全连接尚未建立，所以大大降低了被目标计算机记录的可能性，并且加快了扫描的速度。

（3）FIN 扫描。在前面介绍过的 TCP 报文中，有一个字段为 FIN，FIN 扫描则依靠发送 FIN 来判断目标计算机的指定端口是否活动。

发送一个 FIN=1 的 TCP 报文到一个关闭的端口时，该报文会被丢掉，并返回一个 RST 报文。但是，如果当 FIN 报文到一个活动的端口时，该报文只是简单的丢掉，不会返回任何回应。

从 FIN 扫描可以看出，这种扫描没有涉及任何 TCP 连接部分，因此，这种扫描比前两种都安全，可以称之为秘密扫描。

（4）第三方扫描。第三方扫描又称“代理扫描”，这种扫描是利用第三方主机来代

替入侵者进行扫描。这个第三方主机一般是入侵者通过入侵其他计算机而得到的，该“第三方”主机常被入侵者称之为“肉鸡”。这些“肉鸡”一般为安全防御系数极低的个人计算机。

4.2.7 强化 TCP/IP 堆栈以抵御拒绝服务攻击

针对 TCP/IP 堆栈的攻击方式有多种类型，下面分别介绍攻击原理及抵御方法。

1．同步包风暴（SYN Flooding）

同步包风暴是当前最流行的 DoS 与 DDoS 攻击的方式之一，是应用最广泛的一种 DoS 攻击方式，它的原理虽然简单，但使用起来却十分有效。

问题出在 TCP 连接的三次握手中，假设一个用户向服务器发送了 SYN 报文后突然死机或掉线，那么服务器在发出 SYN＋ACK 应答报文后是无法收到客户端的 ACK 报文的（第三次握手无法完成），这种情况下服务器端一般会重试（再次发送 SYN＋ACK 给客户端）并等待一段时间后丢弃这个未完成的连接，这段时间的长度称为 SYN Timeout，一般来说这个时间是分钟的数量级（大约为 30 秒～2 分钟）。一个用户出现异常导致服务器的一个线程等待 1 分钟并不是什么很大的问题，但如果有一个恶意的攻击者大量模拟这种情况，服务器端将为了维护一个非常大的半连接列表而消耗非常多的资源——数以万计的半连接，即使是简单的保存并遍历也会消耗非常多的 CPU 时间和内存，何况还要不断地对这个列表中的 IP 进行 SYN＋ACK 的重试。实际上，如果服务器的 TCP/IP 堆栈不够强大，最后的结果往往是堆栈溢出崩溃。即使服务器端的系统足够强大，服务器端也将忙于处理攻击者伪造的 TCP 连接请求而无暇理睬客户的正常请求（毕竟客户端的正常请求比率非常小），此时从正常客户的角度来看，服务器失去响应，这种情况称作：服务器端受到了 SYN Flooding 攻击。

如图 4-10 所示，如果攻击者盗用的是某台可达主机 X 的 IP 地址，由于主机 X 没有向主机 D 发送连接请求，所以当它收到来自 D 的 SYN＋ACK 包时，会向 D 发送 RST 包，主机 D 会将该连接重置。因此，攻击者通常伪造主机 D 不可达的 IP 地址作为源地址。攻击者只要发送较少的来源地址经过伪装而且无法通过路由达到的 SYN 连接请求至目标主机提供 TCP 服务的端口，将目的主机的 TCP 缓存队列填满，就可以实施一次成功的攻击。实际情况下，攻击者往往会持续不断地发送 SYN 包，故称为“SYN 洪水”。

可以通过修改注册表防御 SYN Flooding 攻击，修改键值位于注册表项 HKEY LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services 的下面，如表 4-3 所示。

表 4-3 防御 SYN Flooding 所需修改键值

值 名 称	值（REG_DWORD）
SynAttackProtect	2
TcpMaxPortsExhausted	1

续表

值　名　称	值（REG_DWORD）
TcpMaxHalfOpen	500
TcpMaxHalfOpenRetried	400
TcpMaxConnectResponseRetransmissions	2
TcpMaxDataRetransmissions	2
EnablePMTUDiscovery	0
KeepAliveTime	300 000（5 分钟）
NoNameReleaseOnDemand	1

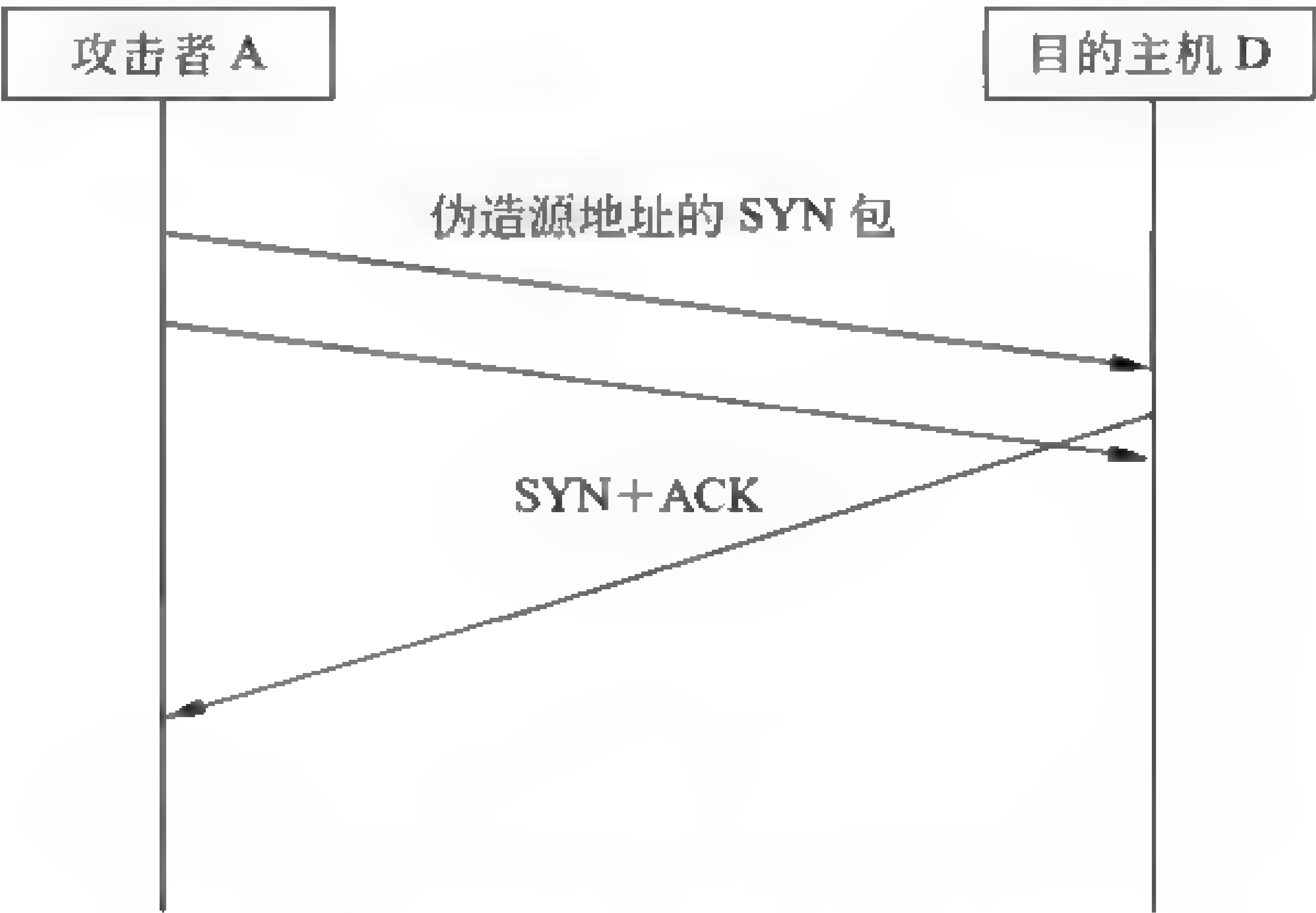


图 4-10　目的主机 D 遭受 SYN 洪水攻击

2．ICMP 攻击

ICMP 协议是 TCP/IP 协议集中的一个子协议，主要用于在主机与路由器之间传递控制信息，包括报告错误、交换受限控制和状态信息等。当遇到 IP 数据无法访问目标、IP 路由器无法按当前的传输速率转发数据包等情况时，会自动发送 ICMP 消息。可以通过 Ping 命令发送 ICMP 回应请求消息并记录收到 ICMP 回应回复消息，通过这些消息来对网络或主机的故障提供参考依据。

ICMP 协议本身的特点决定了它非常容易被用于攻击网络上的路由器和主机。例如，前面提到的 Ping of Death 攻击就是利用操作系统规定的 ICMP 数据包最大尺寸不超过 64KB 这一规定，达到使 TCP/IP 堆栈崩溃、主机死机的效果。

可以通过修改注册表防御 ICMP 攻击，修改键值位于注册表项 HKLM\System\CurrentControlSet\Services\AFD\Parameters 的下面，如表 4-4 所示。

表 4-4　防御 ICMP 所需修改键值

值　名　称	值（REG_DWORD）
EnableICMPRedirect	0

3. SNMP 攻击

SNMP 是 TCP/IP 网络中标准的管理协议，它允许网络中的各种设备和软件，包括交换机、路由器、防火墙，集线器，甚至操作系统、服务器产品和部件等，能与管理软件通信，汇报其当前的行为和状态。但是，SNMP 还能被用于控制这些设备和产品，重定向通信流，改变通信数据包的优先级，甚至断开通信连接。总之，入侵者如果具备相应能力，就能完全接管你的网络。

可以通过修改注册表防御 SNMP 攻击，修改键值位于注册表项 HKLM\System\CurrentControlSet\Services\Tcpip\Parameters 的下面，如表 4-5 所示。

表 4-5 防御 SNMP 所需修改键值

值 名 称	值（REG_DWORD）
EnableDeadGWDetect	0

4.2.8 系统漏洞扫描

系统漏洞扫描是对重要计算机信息系统进行检查，发现其中可能被黑客利用的漏洞。系统漏洞扫描的结果是对系统安全性能的一个评估，指出了哪些攻击是可能的，因此，成为安全方案的一个重要组成部分。目前，系统漏洞扫描从底层技术来划分，可以分为基于网络的扫描和基于主机的扫描这两种类型。

1. 基于网络的漏洞扫描

基于网络的漏洞扫描器，是通过网络来扫描远程计算机中的漏洞。例如，利用低版本的 DNS Bind 漏洞，攻击者能够获取 root 权限，侵入系统或者攻击者能够在远程计算机中执行恶意代码。使用基于网络的漏洞扫描工具，能够监测到这些低版本的 DNS Bind 是否在运行。一般来说，基于网络的漏洞扫描工具可以看作一种漏洞信息收集工具，根据不同漏洞的特性，构造网络数据包，发给网络中的一个或多个目标服务器，以判断某个特定的漏洞是否存在。基于网络的漏洞扫描器，一般由以下几个方面组成。

（1）漏洞数据库模块。漏洞数据库包含了各种操作系统的各种漏洞信息，以及如何检测漏洞的指令。

（2）用户配置控制台模块。用户配置控制台与安全管理员进行交互，用来设置要扫描的目标系统，以及扫描哪些漏洞。

（3）扫描引擎模块。扫描引擎是扫描器的主要部件。根据用户配置控制台部分的相关设置，扫描引擎组装好相应的数据包，发送到目标系统，将接收到的目标系统的应答数据包与漏洞数据库中的漏洞特征进行比较，来判断所选择的漏洞是否存在。

（4）当前活动的扫描知识库模块。通过查看内存中的配置信息，该模块监控当前活动的扫描，将要扫描的漏洞的相关信息提供给扫描引擎。

（5）结果存储器和报告生成工具。报告生成工具，利用当前活动扫描知识库中存储

的扫描结果，生成扫描报告。

基于网络的漏洞扫描器有很多优点。

（1）基于网络的漏洞扫描器的价格相对来说比较便宜。

（2）基于网络的漏洞扫描器在操作过程中，不需要涉及到目标系统的管理员。

（3）基于网络的漏洞扫描器，在检测过程中，不需要在目标系统上安装任何东西。

（4）维护简便。当企业的网络发生了变化时，只要某个节点能够扫描网络中的全部目标系统，则基于网络的漏洞扫描器不需要进行调整。

2．基于主机的漏洞扫描

基于主机的漏洞扫描器，扫描目标系统的漏洞的原理，与基于网络的漏洞扫描器的原理类似，但是，两者的体系结构不一样。基于主机的漏洞扫描器通常在目标系统上安装了一个代理（Agent）或者是服务（Services），以便能够访问所有的文件与进程，这也使得基于主机的漏洞扫描器能够扫描更多的漏洞。

基于主机的漏洞扫描优点如下。

（1）扫描的漏洞数量多。

（2）集中化管理。基于主机的漏洞扫描器通常都有个集中的服务器作为扫描服务器。所有扫描的指令均从服务器进行控制，这一点与基于网络的扫描器类似。服务器下载到最新的代理程序后，再分发给各个代理。这种集中化管理模式，使得基于主机的漏洞扫描器的部署能够快速实现。

（3）网络流量负载小。由于 ESM 管理器与 ESM 代理之间只有通信的数据包，漏洞扫描部分都由 ESM 代理单独完成，这就大大减少了网络的流量负载。当扫描结束后，ESM 代理再次与 ESM 管理器进行通信，将扫描结果传送给 ESM 管理器。

4.3　防火墙应用配置

4.3.1　防火墙技术概述

1．防火墙的定义

防火墙的本义是指古代构筑和使用木制结构房屋的时候，为防止火灾的发生和蔓延，人们将坚固的石块堆砌在房屋周围作为屏障，这种防护构筑物就被称之为“防火墙”。其实与防火墙一起起作用的就是“门”。如果没有门，各房间的人如何沟通呢，这些房间的人又如何进出呢？当火灾发生时，这些人又如何逃离现场呢？这个门就相当于计算机网络防火墙中的“安全策略”。

防火墙是设置在两个或多个网络之间的安全阻隔，用于保证本地网络资源的安全，通常是包含软件部分和硬件部分的一个系统或多个系统的组合。内部网络被认为是安全和可信赖的，而外部网络（通常是 Internet）被认为是不安全和不可信赖的。防火墙的作

用是通过允许、拒绝或重新定向经过防火墙的数据流，防止不希望的、未经授权的通信进出被保护的内部网络，并对进、出内部网络的服务和访问进行审计和控制，本身具有较强的抗攻击能力，并且只有授权的管理员方可对防火墙进行管理，通过边界控制来强化内部网络的安全。防火墙在网络中的位置通常如图 4-11 所示。

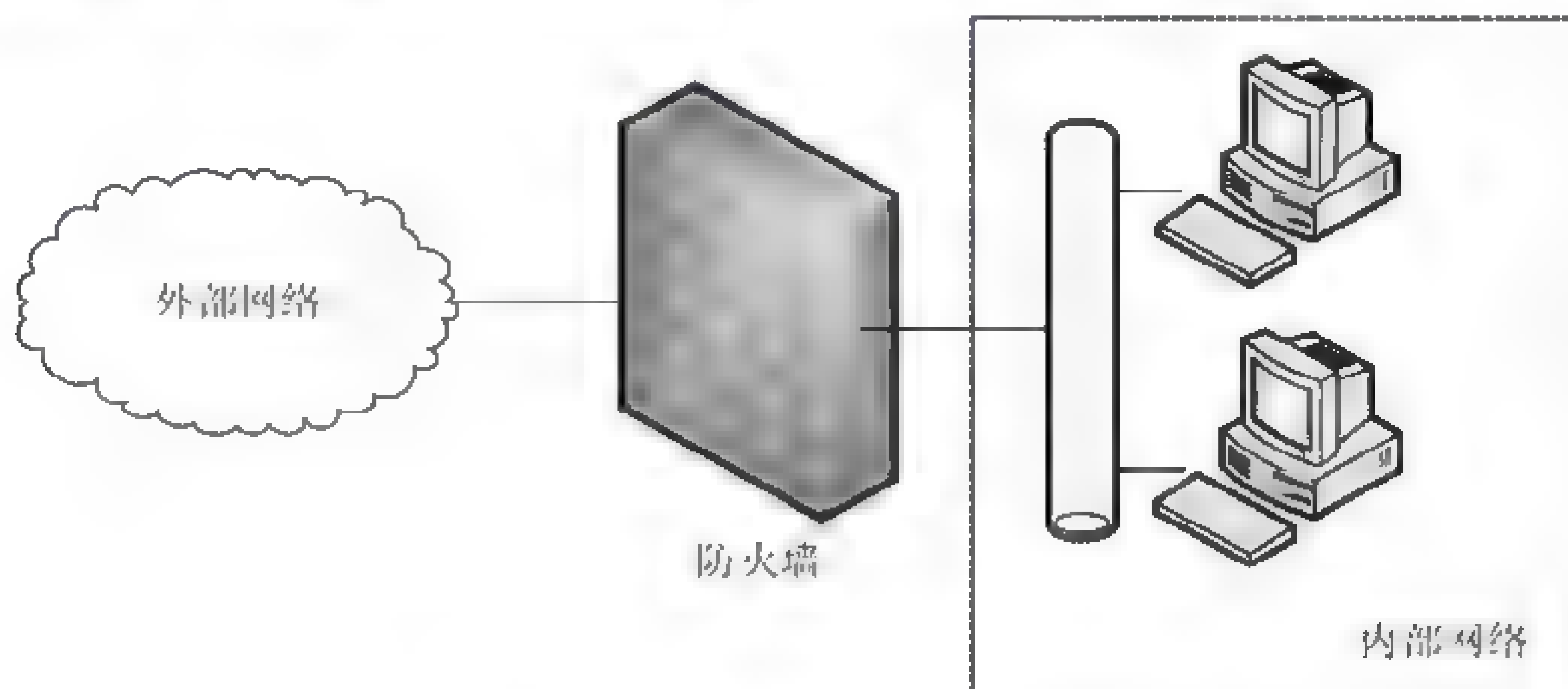


图 4-11 防火墙在网络中的位置

如果没有防火墙，则整个内部网络的安全性完全依赖于每个主机，因此，所有的主机都必须达到一致的高度安全水平。也就是说，网络的安全水平是由最低的那个安全水平的主机决定的，这就是所谓的"木桶原理"，木桶能装多少水由最低的地方决定。网络越大，对主机进行管理使它们达到统一的安全级别水平就越不容易。

防火墙隔离了内部网络和外部网络，它被设计为只运行专用的访问控制软件的设备，而没有其他的服务，因此也就意味着相对少一些缺陷和安全漏洞。此外，防火墙也改进了登录和监测功能，从而可以进行专用的管理。如果采用了防火墙，内部网络中的主机将不再直接暴露给来自 Internet 的攻击。因此，对整个内部网络的主机的安全管理就变成了防火墙的安全管理，这样就使安全管理变得更为方便，易于控制，也会使内部网络更加安全。

防火墙一般安放在被保护网络的边界，必须做到以下几点，才能使防火墙起到安全防护的作用。

（1）所有进出被保护网络的通信都必须通过防火墙。

（2）所有通过防火墙的通信必须经过安全策略的过滤或者防火墙的授权。

（3）防火墙本身是不可侵入的。

总之，防火墙是在被保护网络和非信任网络之间进行访问控制的一个或一组访问控制部件。它是一种逻辑隔离部件，而不是物理隔离部件，它所遵循的原则是：在保证网络畅通的情况下，尽可能地保证内部网络的安全。防火墙是在已经制定好的安全策略下进行访问控制，所以一般情况下它是一种静态安全部件。但随着防火墙技术的发展，防火墙或通过与 IDS（入侵检测系统）进行联动，或自身集成 IDS 功能，将能够根据实际

的情况进行动态的策略调整。

2．防火墙的分类及技术

了解什么是防火墙之后，可以对当前市场上的防火墙进行一下分类。目前防火墙产品非常多，划分的标准也比较纷杂，主要是以防火墙软硬件形式和防火墙采用的技术为参照物进行划分。

1）按防火墙的软硬件形式分类

如果按防火墙的软、硬件形式进行分类，防火墙可以分为硬件防火墙、软件防火墙和嵌入式防火墙。

（1）基于硬件的防火墙。是一个已经预装有软件的硬件设备。基于硬件的防火墙又可分为家庭办公型和企业型两种款式。防火墙在外观上与平常我们所见到的集线器和交换机类似，只是只有少数几个接口，分别用于连接内、外部网络，那是由防火墙的基本作用决定的。

（2）基于软件的防火墙。是能够安装在操作系统和硬件平台上的防火墙软件包。如果用户的服务器装有企业级操作系统，购买基于软件的防火墙则是合理的选择。如果用户是一家小企业，并且想把防火墙与应用服务器（如网站服务器）结合起来，配备一个基于软件的防火墙不失为明智之举。

国内外还有许多网络安全软件厂商开发出面向家庭用户的基于纯软件的防火墙，俗称“个人防火墙”。之所以说它是“个人防火墙”，是因为它是安装在主机中，只对一台主机进行防护，而不是保护整个网络。

（3）嵌入式防火墙。就是内嵌于路由器或交换机的防火墙。嵌入式防火墙是某些路由器的标准配置。用户也可以购买防火墙模块，安装到已有的路由器或交换机中。嵌入式防火墙也被称为检查点防火墙。由于因特网使用的协议多种多样，所以不是所有的网络服务都能得到嵌入式防火墙的有效处理。嵌入式防火墙工作于 IP 层，无法保护网络免受病毒、蠕虫和特洛伊木马程序等来自应用层的威胁。就本质而言，嵌入式防火墙常常是无监控状态的，它在传递信息包时并不考虑以前的连接状态。

2）按防火墙采用的技术分类

防火墙技术可根据防范的方式和侧重点的不同分为包过滤型防火墙、应用层网关、代理服务型防火墙三种类型。

（1）包过滤（packet filtering）型防火墙。工作在 OSI 网络参考模型的网络层和传输层，它根据数据包头源地址、目的地址、端口号和协议类型等标志确定是否允许数据包通过。只有满足过滤条件的数据包才被转发到相应的目的地，其余数据包则被从数据流中丢弃。

包过滤方式是一种通用、廉价和有效的安全手段。之所以通用，是因为它不是针对各个具体的网络服务采取特殊的处理方式，适用于所有网络服务；之所以廉价，是因为大多数路由器都提供数据包过滤功能，所以这类防火墙多数是由路由器集成的；之所以

有效，是因为它能在很大程度上满足绝大多数企业安全要求。

包过滤方式的优点是不用改动客户机和主机上的应用程序，因为它工作在网络层和传输层，与应用层无关。但其弱点也是明显的：过滤判别的依据只是网络层和传输层的有限信息，因而各种安全要求不可能充分满足；在许多过滤器中，过滤规则的数目是有限制的，且随着规则数目的增加，性能会受到很大地影响；由于缺少上下文关联信息，不能有效地过滤如 UDP、RPC 一类的协议。另外，大多数过滤器中缺少审计和报警机制，它只能依据包头信息，而不能对用户身份进行验证，很容易受到“地址欺骗型”攻击。包过滤型防火墙对安全管理人员素质要求高，建立安全规则时，必须对协议本身及其在不同应用程序中的作用有较深入的理解。

（2）应用层网关防火墙。应用层网关（Application Level Gateways）防火墙是在 OSI/RM 应用层上建立协议过滤和转发功能。它针对特定的网络应用服务协议使用指定的数据过滤逻辑，并在过滤的同时，对数据包进行必要的分析、登记和统计，并形成报告提供给网络安全管理员作进一步分析。

数据包过滤和应用层网关防火墙有一个共同的特点，就是它们仅仅依靠特定的逻辑判定是否允许数据包通过。一旦满足逻辑，则防火墙内外的计算机系统建立直接联系，防火墙外部的用户便有可能直接了解防火墙内部的网络结构和运行状态，这有利于实施非法访问和攻击。

（3）代理服务型防火墙。代理服务型（Proxy Service）防火墙是针对数据包过滤和应用层网关技术存在的缺点而引入的防火墙技术，其特点是将所有跨越防火墙的网络通信链路分为两段。防火墙内外计算机系统间不能直接连接，都要通过代理服务型防火墙中转连接。外部计算机的网络链路只能到达代理服务型防火墙，从而起到了隔离防火墙内外计算机系统的作用。有些网络安全专业人员将代理服务型防火墙归于应用层网关一类。

代理服务型防火墙最突出的优点就是安全。由于它工作于最高层，所以可以对网络中任何一层数据通信进行筛选保护，而不是像包过滤那样，只是对网络层的数据进行过滤。

另外，代理服务型防火墙采取的是一种代理机制，它可以为每一种应用服务建立一个专门的代理，所以内外部网络之间的通信不是直接的，而都需先经过代理服务器审核，通过后再由代理服务器代为连接，根本没有给内、外部网络计算机任何直接会话的机会，从而避免了入侵者使用数据驱动类型的攻击方式入侵内部网。包过滤类型的防火墙则很难彻底避免这一漏洞。

有优点就有缺点，任何事物都一样。代理服务型防火墙的最大缺点就是速度相对比较慢，当用户对内外部网络网关的吞吐量要求比较高时，代理服务型防火墙就会成为内外部网络之间的瓶颈。由于防火墙需要为不同的网络服务建立专门的代理服务，在自己的代理程序为内、外部网络用户建立连接时需要时间，所以给系统性能带来了一些负面

影响，但通常不会太明显。

4.3.2　防火墙体系结构

防火墙的经典体系结构主要有三种形式：双重宿主主机体系结构、被屏蔽主机体系结构和被屏蔽子网体系结构。在介绍防火墙的体系结构之前，先介绍防火墙体系结构中几个常见的术语。

（1）堡垒主机：是指可能直接面对外部用户攻击的主机系统，在防火墙体系结构中，特指那些处于内部网络的边缘，并且暴露于外部网络用户面前的主机系统。一般来说，堡垒主机上提供的服务越少越好，因为每增加一种服务就增加了被攻击的可能性。

（2）双重宿主主机：是指通过不同网络接口连入多个网络的主机系统，又称为多穴主机系统。一般来说，双重宿主主机是实现多个网络之间互连的关键设备，如网桥是在数据链路层实现互连的双重宿主主机，路由器是在网络层实现互连的双重宿主主机，应用层网关是在应用层实现互连。

（3）周边网络：是指在内部网络、外部网络之间增加的一个网络，一般来说，对外提供服务的各种服务器都可以放在这个网络里。周边网络也被称为非武装区域（Demilitarized Zone，DMZ）。周边网络的存在，使得外边用户访问服务器时不需要进入内部网络，而内部网络用户对服务器维护工作导致的信息传递也不会泄露至外部网络。同时，周边网络与外部网络或内部网络之间存在着数据包过滤，这样为外部用户的攻击设置了多重障碍，确保了内部网络的安全。

1．双重宿主主机体系结构

防火墙的双重宿主主机体系结构是指以一台双重宿主主机作为防火墙系统的主体，执行分离外部网络与内部网络的任务。一个典型的双重宿主主机体系结构如图 4-12 所示。

在基于双重宿主主机体系结构的防火墙中，带有内部网络和外部网络接口主机系统构成了防火墙的主体，该台双重宿主主机具备了成为内部网络和外部网络之间路由器的条件，但是在内部网络与外部网络之间进行数据包转发的进程是被禁止运行的。为了达到防火墙的基本效果，在双重宿主主机体系结构中，任何路由功能是禁止的，甚至数据包过滤技术也是不允许在双重宿主主机上实现的。双重宿主主机唯一可以采用的防火墙技术就是应用层代理，内部网络用户可以通过客户端代理软件以代理方式访问外部网络资源，或者直接登录至双重宿主主机成为一个用户，再利用该主机访问外部资源。

双重宿主主机体系结构防火墙的优点在于网络结构比较简单，由于内、外网络之间没有直接的数据交互而较为安全；内部用户账号的存在可以保证对外部资源进行有效控制；由于应用层代理机制的采用，可以方便地形成应用层的数据与信息过滤。其缺点在于，用户访问外部资源较为复杂，如果用户需要登录到主机上才能访问外部资源，则主机的资源消耗较大；用户机制存在安全隐患，并且内部用户无法借助于该体系结构访问新的服务或者特殊服务；一旦外部用户入侵了双重宿主主机，则导致内部网络处于不安

全状态。

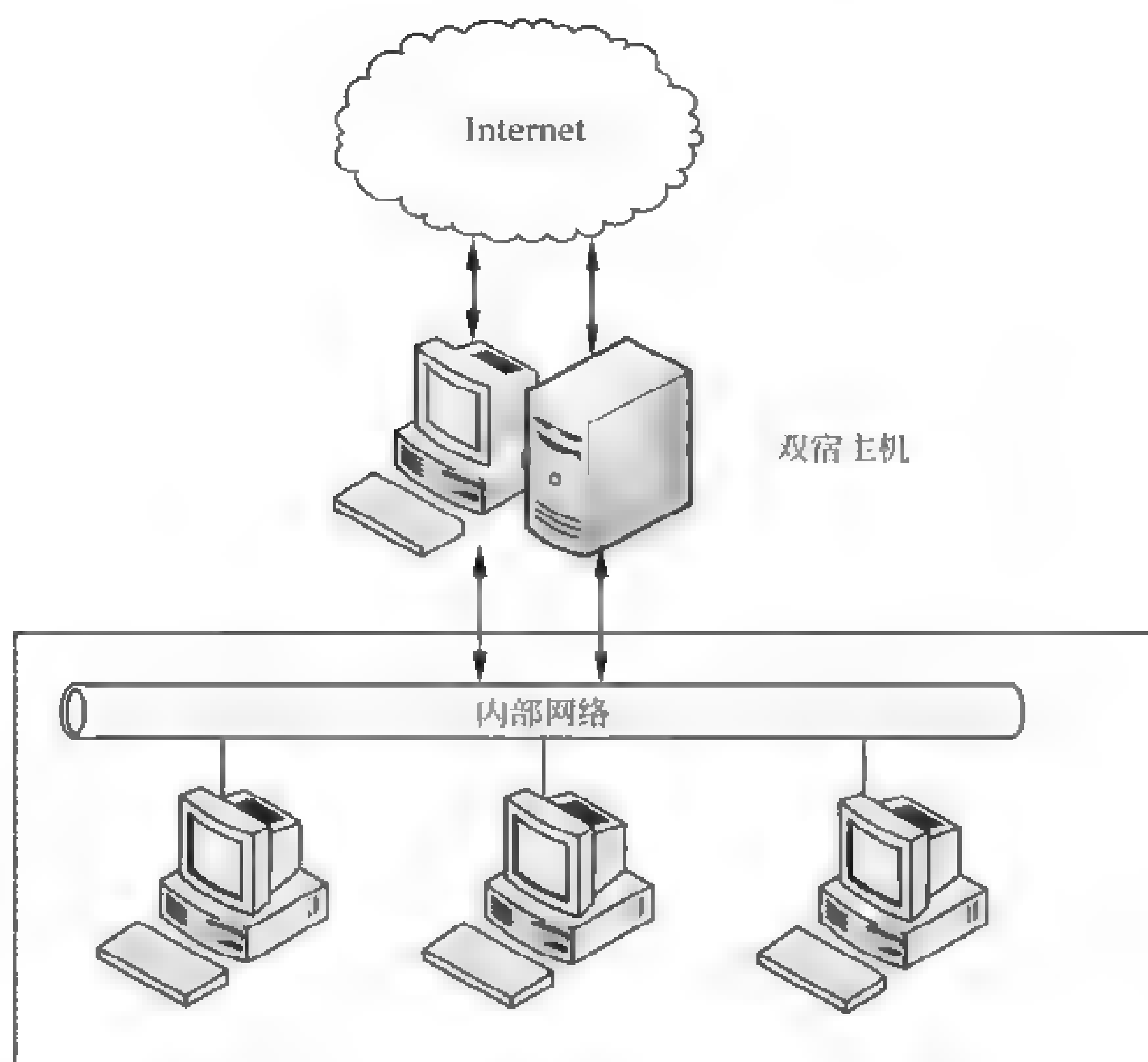


图 4-12 双重宿主主机防火墙体系结构

2．被屏蔽主机体系结构

被屏蔽主机体系结构是指通过一个单独的路由器和内部网络上的堡垒主机共同构成防火墙，主要通过数据包过滤实现内部、外部网络的隔离和对内网的保护。一个典型的被屏蔽主机体系结构如图 4-13 所示。

在被屏蔽主机体系结构中，有两道屏障，一道是屏蔽路由器，另一道是堡垒主机。

屏蔽路由器位于网络的最边缘，负责与外网实施连接，并且参与外网的路由计算。屏蔽路由器不提供任何服务，仅提供路由和数据包过滤功能，因此屏蔽路由器本身较为安全，被攻击的可能性较小。由于屏蔽路由器的存在，使得堡垒主机不再是直接与外网互连的双重宿主主机，增加了系统的安全性。

堡垒主机存放在内部网络中，是内部网络中唯一可以连接到外部网络的主机，也是外部用户访问内部网络资源必须经过的主机设备。在经典的被屏蔽主机体系结构中，堡垒主机也通过数据包过滤功能实现对内部网络的防护，并且该堡垒主机仅仅允许通过特定的服务连接。主机也可以不提供数据包过滤功能，而是提供代理功能，内部用户只能通过应用层代理访问外部网络，而堡垒主机就成为外部用户唯一可以访问的内部主机。

被屏蔽主机体系结构的优点如下。

（1）被屏蔽主机体系结构比双重宿主主机体系结构具有更高的安全特性。由于屏蔽路由器在堡垒主机之外提供数据包过滤功能，使得堡垒主机要比双重宿主主机相对安全，

存在漏洞的可能性较小，被攻击的可能性也较小。同时，堡垒主机的数据包过滤功能限制外部用户只能访问内部特定主机上的特定服务，或者只能访问堡垒主机上的特定服务，在提供服务的同时仍然保证了内部网络的安全。

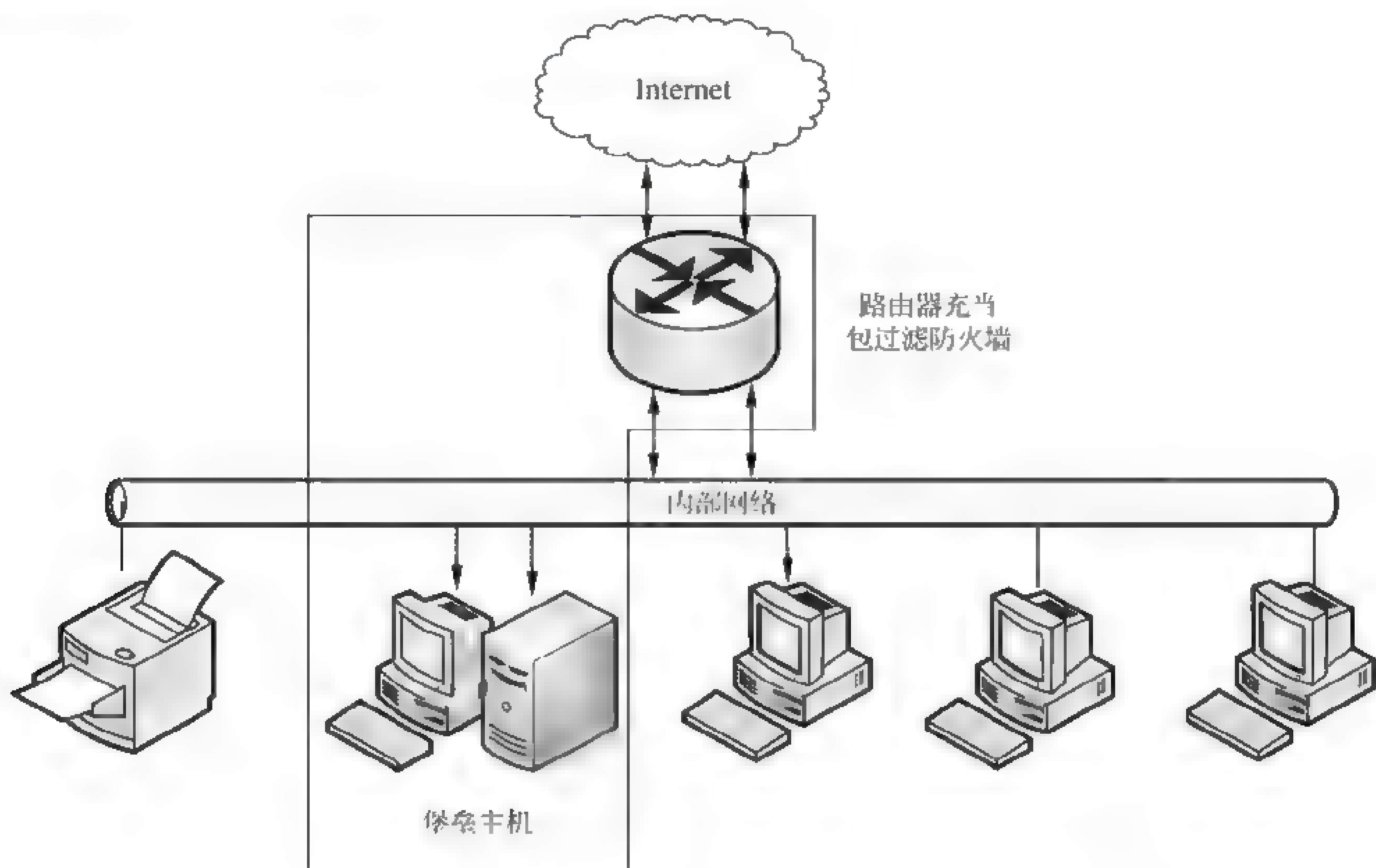


图 4-13　被屏蔽主机防火墙体系结构

（2）内部网络用户访问外部网络较为方便、灵活，在被屏蔽路由器和堡垒主机不允许内部用户直接访问外部网络，则用户通过堡垒主机提供的代理服务访问外部资源。在实际应用中，可以将两种方式综合运用，访问不同的服务采用不同的方式。例如，内部用户访问 WWW，可以采用堡垒主机的应用层代理，而一些新的服务可以直接访问。

（3）由于堡垒主机和屏蔽路由器同时存在，使得堡垒主机可以从部分安全事务中解脱出来，从而可以以更高的效率提供数据包过滤或代理服务。

被屏蔽主机体系结构的缺点如下。

（1）在被屏蔽主机体系结构中，外部用户在被允许的情况下可以访问内部网络，这样存在一定安全隐患。

（2）与双重宿主主机体系一样，一旦用户入侵堡垒主机，就会导致内部网络处于不安全状态。

（3）路由器和堡垒主机的过滤规则配置较为复杂，较容易形成错误和漏洞。

3．被屏蔽子网体系结构

在防火墙的双重宿主主机体系结构和被屏蔽子网体系结构中，主机都是最主要的安

全缺陷，一旦主机被入侵，则整个网络都处于入侵者的威胁之中，为解决这种安全隐患，出现了屏蔽子网体系结构。

被屏蔽子网体系结构将防火墙的概念扩充至一个由两台路由器包围起来的特殊网络——周边网络，并且将容易受到攻击的堡垒主机都置于这个周边网络中。一个典型的被屏蔽子网体系结构如图 4-14 所示。

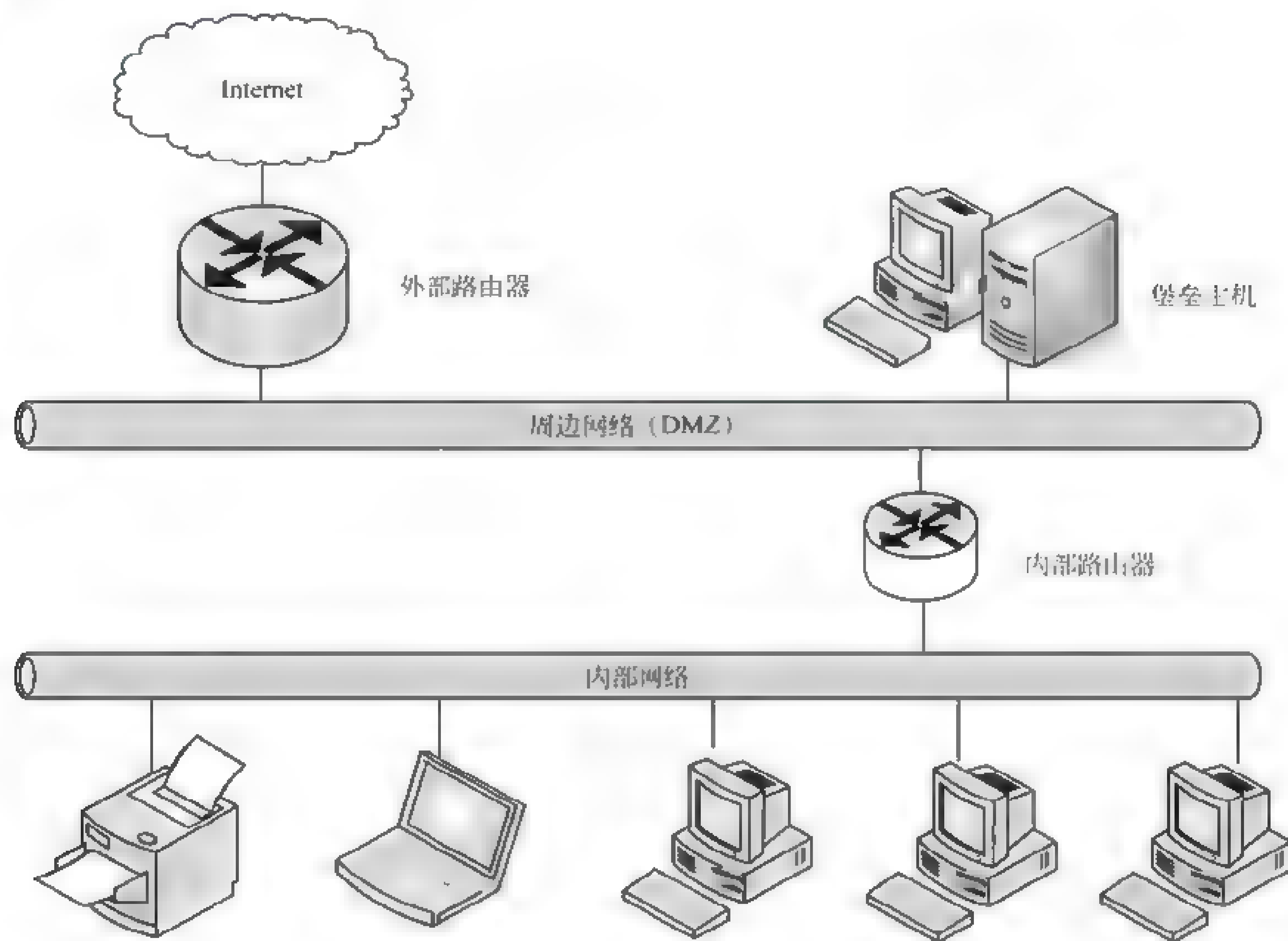


图 4-14 被屏蔽子网防火墙体系结构

被屏蔽子网体系结构的防火墙比较复杂，主要由 4 个部件组成，分别为周边网络、外部路由器、内部路由器以及堡垒主机。

（1）周边网络。周边网络是位于非安全、不可信的外部网络与安全、可信的内部网络之间的一个附加网络。周边网络与外部网络、周边网络与内部网络之间都是通过屏蔽路由器实现逻辑隔离的，因此，外部用户必须穿越两道屏蔽路由器才能访问内部网络。一般情况下，外部用户不能访问内部网络，仅能够访问周边网络中的资源。由于内部用户间通信的数据包不会通过屏蔽路由器传递至周边网络，外部用户即使入侵了周边网络中的堡垒主机，也无法监听到内部网络的信息。

（2）外部路由器。外部路由器的主要作用在于保护周边网络和内部网络，是屏蔽子网体系结构的第一道屏障。在其上设置了对周边网络和内部网络进行访问的过滤规则，该规则主要针对外网用户，例如，限制外网用户仅能访问周边网络而不能访问内部网络，

或者仅能访问内部网络的部分主机。外部路由器基本上对周边网络发出的数据包不进行过滤，因为周边网络发送的数据包都来自于堡垒主机或由内部路由器过滤后的内部主机数据包。外部路由器上应该复制内部服务器上的规则，以避免内部路由器失效的负面影响。

（3）内部路由器。内部路由器用于隔离周边网络和内部网络，是屏蔽子网体系结构的第二道屏障。在其上设置了针对内部用户的访问过滤规则，对内部用户访问周边网络和外部网络进行限制，例如，部分内部网络用户只能访问周边网络而不能访问外边网络等。内部路由器复制了外边路由器的内网过滤规则，以防止外部路由器的过滤功能失效的严重后果。内部路由器还要限制周边网络的堡垒主机和内部网络之间的访问，以减轻在堡垒主机被入侵后可能影响的内部主机数量和服务的数量。

（4）保垒主机。在被屏蔽子网体系结构中，堡垒主机位于周边网络，可以向外部用户提供 WWW、FTP 等服务，接受来自外部网络用户的服务资源访问请求。同时，堡垒主机也可以向内部网络用户提供 DNS、电子邮件、WWW 代理和 FTP 代理等多种服务，提供内部网络用户访问外部资源的接口。

与双重宿主主机体系结构和被屏蔽子网体系结构相比较，被屏蔽子网体系结构具有明显的优越性，这些优越性体现在如下几个方面。

（1）由外部路由器和内部路由器构成了双层防护体系，入侵者难以突破。

（2）外部用户访问服务资源时无需进入内部网络，在保证服务的情况下提高了内部网络安全性。

（3）外部路由器和内部路由器上的过滤规则复制避免了路由器失效产生的安全隐患。

（4）堡垒主机由外部路由器的过滤规则和本机安全机制共同防护，用户只能访问堡垒主机提供的服务。

（5）即使入侵者通过堡垒主机提供服务中的缺陷控制了堡垒主机，由于内部防火墙将内部网络和周边网络隔离，入侵者也无法通过监听周边网络获取内部网络信息。

被屏蔽子网体系结构的缺点如下。

（1）构建被屏蔽子网体系结构的成本较高。

（2）被屏蔽子网体系结构的配置较为复杂，容易出现配置错误导致的安全隐患。

4．其他体系结构

除了经典的三种体系结构之外，防火墙还存在着多种经典结构的变化形式，这些变化形式主要是针对被屏蔽子网体系结构的扩展，在不同的网络环境和不同的安全需求下的运用。这些体系结构的变化包括以下内容。

（1）合并内部和外部路由器。

（2）合并堡垒主机和外部路由器。

（3）合并堡垒主机和内部路由器。

（4）多台内部路由器。

（5）多台外部路由器。

（6）多个周边网络。

4.3.3 分布式防火墙技术

1．分布式防火墙技术产生的背景

传统的边缘防火墙只对企业网络的周边提供保护。边缘防火墙对从外部网络进入企业内部局域网的流量进行过滤和审查，它们并不能确保企业内部网络用户之间的安全访问。据统计，60%的攻击和越权访问来自内部，边界防火墙在对付网络内部威胁时束手无策。因为传统的边界式防火墙设置一般都基于 IP 地址，因而一些内部主机和服务器的 IP 地址的变化将导致设置文件中的规则改变，也就是说，这些规则的设定受到网络拓扑的制约。随着 IP 安全协议（如 IPSec、SSH 和 SSL 等）的逐渐实现，如果分处内部网络和外部网络的两台主机采用 IP 安全协议进行端到端的通信（其实以上所介绍的 SSL VPN 就是这样一种端到端通信的应用），防火墙由于没有相应的密钥而无法看到 IP 包的内容，因而也就无法对其进行过滤。由于防火墙假设内部网络的用户可信任，一旦有内部主机被侵入，通常容易扩展该次攻击。对于这些问题，传统意义上的防火墙是很难解决的。

另外，由于边界式防火墙把检查机制集中在网络边界处的单点上，产生了网络的瓶颈和单点故障隐患。从性能的角度来说，防火墙极易成为网络流量的瓶颈。

基于此，一种新型的防火墙技术——分布式防火墙（distributed firewalls）技术产生了。它可以很好地解决边界防火墙以上的不足，当然不是对每台主机安装防火墙，而是把防火墙的安全防护系统延伸到网络中的各台主机。该技术一方面保证用户的投资不会很高，另一方面给网络所带来的安全防护是非常全面的。

2．分布式防火墙的结构

分布式防火墙负责对网络边界、各子网和网络内部各节点之间的安全防护，根据其所需完成的功能，分布式防火墙的体系结构包含如下部分。

（1）网络防火墙（network firewall）。用于内部网与外部网之间，以及内部网各子网之间的防护。在功能上与传统的边界式防火墙类似，但与传统边界防火墙相比，它多了一种用于对内部子网之间的安全防护层，这样整个网络的安全防护体系就显得更加全面，更加可靠。

（2）主机防火墙（host firewall）。用于对网络中的服务器和桌面机进行防护，达到了应用层的安全防护，比起网络层更加彻底。这是传统边界式防火墙所不具有的，是对传统边界式防火墙在安全体系方面的一个完善。

（3）中心管理系统（central management system）。这是分布式防火墙管理器软件，负责总体安全策略的策划、管理、分发及日志的汇总。提高了防火墙的安全防护灵活性，同时具备高可管理性。

3．分布式防火墙的主要特点

（1）主机驻留。分布式防火墙的最重要特征是驻留在被保护的主机上，该主机以外的网络不管是处在网络内部还是网络外部都认为是不可信任的，因此可以针对该主机上运行的具体应用和对外提供的服务设定针对性很强的安全策略。使得安全策略不仅仅停留在网络与网络之间，而是把安全策略推广延伸到每个网络末端。

（2）嵌入操作系统内核。这主要是针对纯软件式的分布式防火墙而言的。操作系统自身存在许多安全漏洞是众所周知的。纯软件式的分布式主机防火墙也运行在主机上，所以其运行机制是主机防火墙的关键技术之一。为自身的安全和彻底堵住操作系统的漏洞，主机防火墙的安全监测核心引擎要以嵌入操作系统内核的形态运行，直接接管网卡，在把所有数据包进行检查后再提交操作系统。

（3）安全策略的统一管理与部署。针对桌面应用的主机防火墙安全策略由整个系统的管理员统一安排和设置，除了对该桌面机起到保护作用外，也可以对该桌面机的对外访问加以控制，并且这种安全机制是桌面机的使用者不可见和不可改动的。主机防火墙、网络防火墙、统一的安全策略管理中心三者共同构成一个面向企业级客户的整体安全防护系统中不可分割的部分，整个系统的安全检查机制分散布置在整个分布式防火墙体系中。

4．分布式防火墙的主要优势

在新的安全体系结构下，分布式防火墙代表新一代防火墙技术的潮流，它可以在网络的任何交界和节点处设置屏障，从而形成了一个多层次、多协议，内外皆防的全方位安全体系。主要优势如下。

（1）增强了系统安全性。增加了针对主机的入侵检测和防护功能，加强了对来自内部攻击的防范，可以实施全方位的安全策略。由于分布式防火墙将防火墙功能分布到网络的各个子网、桌面系统以及服务器上，从而使企业网络避免发生由于某一节点系统的入侵而导致入侵向整个网络蔓延的情况，同时也使通过公共账号登录网络的用户无法进入那些限制访问的计算机系统。弥补了边界式防火墙对内部网络安全性防范的不足。另外，由于分布式防火墙使用了 IP 安全协议，能够很好地识别在各种安全协议下的内部主机之间的端到端网络通信，使各主机之间的通信得到了很好的保护。所以分布式防火墙有能力防止各种类型的攻击。

（2）提高了系统性能。传统防火墙由于拥有单一的接入控制点，无论对网络的性能还是对网络的可靠性都有不利的影响。分布式防火墙则从根本上去除了单一的接入点，而使这一问题迎刃而解。另一方面，分布式防火墙可以针对各个服务器及终端计算机的不同需要，对防火墙进行最佳配置，配置时能够充分考虑到这些主机上运行的应用，如此便可在保障网络安全的前提下大大提高网络运转效率。

（3）系统的扩展性。因为分布式防火墙分布在整个企业的网络或服务器中，所以它具有无限制的扩展能力。随着网络的增长，它们的处理负荷也在网络中进一步分布，因

此它们的高性能可以持续保持住。而不会像边界式防火墙一样随着网络规模的增大而不堪重负。

（4）实施主机策略。对网络中的各节点可以起到更安全的防护。现在防火墙大多缺乏对主机意图的了解，通常只能根据数据包的外在特性来进行过滤控制。虽然代理型防火墙能够解决该问题，但它需要对每一种协议单独地编写代码，其局限性也是显而易见的。事实上，攻击者很容易伪装成合法包发动攻击，攻击包除了内容以外的部分可以完全与合法包一样。分布式防火墙由主机来实施策略控制，毫无疑问主机对自己的意图有足够的了解，所以分布式防火墙依赖主机做出合适的决定就能很自然地解决这一问题。

（5）应用更为广泛，支持 VPN 通信。分布式防火墙最重要的优势在于，它能够保护物理拓扑上不属于内部网络，但位于逻辑上的“内部”网络的那些主机，这种需求随着 VPN 的发展越来越多。分布式防火墙的建立本身就是基于逻辑网络的概念，因此对它而言，远程内部主机与物理上的内部主机没有任何区别。

4.3.4 防火墙应用规则

有人认为防火墙的部署很简单，只需要把防火墙的 LAN 端口与企业局域网线路连接，把防火墙的 WAN 端口连接到外部网络线路即可。其实这是非常错误的，防火墙的具体部署方法要根据实际的应用需求而定，不是统一的。本节将向大家介绍防火墙的几种典型应用中的部署方法，当然这里所说的防火墙均是特指企业用的硬件防火墙。不过在此之前先要介绍采用堡垒主机的方式实现防火墙用途的几种部署方式。

尽管防火墙主要用于网络边界，但它与路由器一样，同样可应用于内网之中，起到隔离内网关键部门、子网或用户的目的。这样一来，硬件防火墙在网络中的应用主要有以下几个方面。

（1）控制因特网用户对内部网络的访问。

（2）控制局域网内部不同部门网络之间的访问。

（3）控制对服务器中心的网络访问。

1. 企业网络体系结构

1）企业网络体系结构中的三个区域

在企业网络体系结构中，通常有三个区域。

（1）边界网络。此网络通过路由器直接面向 Internet，应该以基本网络通信筛选的形式提供初始层面的保护。它通过外围防火墙将数据转发到外围网络。

（2）外围网络。此网络通常称为 DMZ 或者边缘网络，将用户连接到 Web 服务器或其他服务器。然后，Web 服务器通过内部防火墙连接到内部网络。

（3）内部网络。内部网络则连接各个内部服务器（如企业 OA 服务器、数据库服务器、ERP 服务器和 PDM 服务器等）和内部用户。

2）企业组织中的防火墙及其功能

在企业组织中，常常有两个不同的防火墙——外围防火墙和内部防火墙，网络系统结构如图 4-15 所示。虽然这些防火墙的任务相似，但是它们有不同的侧重点，因为外围防火墙主要提供对不受信任的外部用户的限制，而内部防火墙主要防止外部用户访问内部网络并且限制内部用户可以执行的操作。

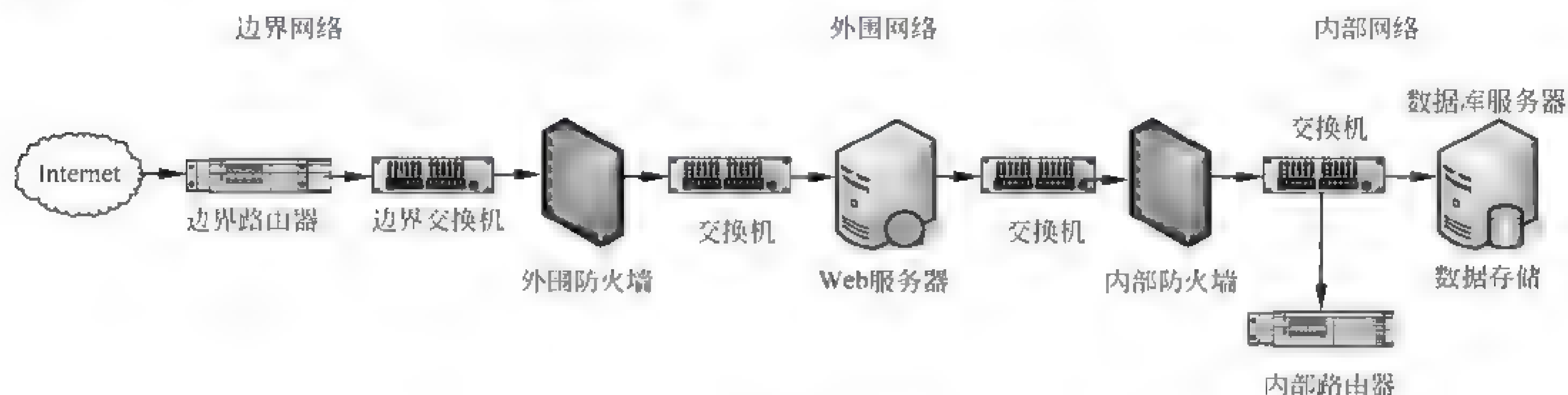


图 4-15 企业网络体系结构

防火墙检查传入的 IP 数据包并且阻止那些检测为入侵性质的数据包。可以通过在默认情况下将某些数据包标识为非法的来完成某些阻挡。或者，也可以将防火墙配置为阻止某些数据包。TCP/IP 协议设计时没有考虑到任何有关窃取或入侵的因素，并且有许多弱点。例如，ICMP 协议设计为 TCP/IP 内的一个消息机制，但是这很容易导致滥用，并且可能导致诸如拒绝服务攻击等问题。内部防火墙比外围防火墙具有更严格的要求。这是因为内部通信的合法目的地可能是内部网络中的任何服务器，因而更加难以控制。

3）选择防火墙时要考虑的因素

有许多种类型的防火墙，在一定程度上是按价格区分的，但是也可以按功能和性能区分。通常，防火墙的价格越贵，能力和功能越好。在选择防火墙之前，应该考虑注意的事项包括预算、现有设备、可用性、可扩展性和所需的功能。

（1）预算方面的考虑。网络环境中的每个防火墙应该在保持经济、有效的同时提供尽可能高级别的服务，但是如果防火墙过分受成本限制，应预先估计这可能会对企业造成潜在的损失。因此在做预算时，应考虑企业网络服务因遭受拒绝服务攻击而被中断时的停机时间成本。

（2）现有设备的考察。此外，需要考虑企业中是否有可以用来节约成本的现有设备。环境中可能有可以重新利用的防火墙和可以安装防火墙功能模块的路由器。

（3）可用性的考虑。可用性的考虑包括：组织需要防火墙在所有的时间都可用吗？如果要提供一个 24×7 小时持续服务的开放 Web 服务器设备，那么将需要 99.999%的可靠性。任何防火墙总会有发生故障的可能性，那么如何减少故障呢？防火墙的可用性可以通过两种方法来改进。

① 冗余部件：为某些很可能发生故障的部件（如电源）配置备用系统，这可以改进防火墙的可用性。因为如果第一个组件发生故障，不会对运营造成任何影响。低成本防火墙通常不具有任何冗余选项。

② 备用设备：为防火墙配置备用系统可以提供一个具有完全适应性的系统，但这需要较高的成本。当然，另一个好处是采用多台防火墙提高可用性的同时，配置负载均衡以便提高网络的性能。

（4）可扩展性的考虑。可扩展性的考虑是指防火墙是否易于扩展其功能模块，当企业网络增加新的网络出口时，防火墙是否能通过增加模块来支持更多的接口。当网络流量快速增长时，防火墙会不会成为网络的瓶颈，这些未来的扩展需求都应该纳入考虑。

（5）所需功能的考虑。所需功能的考虑是指需要防火墙具备哪些功能？如是否支持防御 DoS/DDoS，是否支持 VPN，是否支持 SNMPv3 协议，能否保护特定主机的特定服务等。

2．控制因特网用户对内部网络的访问

控制因特网用户对内部网络的访问是防火墙的一种最基本、最广泛的应用。在这种应用环境下，防火墙位于企业内部局域网与因特网之间，主要保护内部网络不遭受因特网用户的攻击。目前绝大多数中小型企业，采用防火墙的主要目的就是防止外部攻击。

1）网络结构中划分不同的安全级别

在这种应用中，整个网络结构分为三个不同级别的安全区域。

（1）内部网络。内部网络是防火墙重点保护的对象，包括全部的企业内部网络设备及用户主机。不过要注意的是，它是从总体上来进行保护的，因为它位于内、外部网络出/入口之间，不针对具体的主机。这个区域是防火墙的可信区域，由内网用户发出的通信连接默认是无需过滤和审计的。

（2）外部网络。外部网络是防火墙要防备的对象，包括外部因特网用户主机和设备。这个区域为防火墙的非可信网络区域，外部网络用户发起的通信连接必须按照防火墙的安全过滤规则进行过滤和审计，不符合条件的则不允许连接，起到保护内网的目的。

（3）DMZ 区域。DMZ 区域是从企业内部网络中划分出来的一个逻辑区域，其中包括内部网络中用于公众服务的外部服务器，如 Web 服务器、邮件服务器、FTP 服务器和外部 DNS 服务器等，都是为因特网公众用户提供某种信息服务的。在这个区域中的网络受保护的级别较低，需要对外开放某些特定的服务和应用，因为如果级别太高，这些提供公共服务的网络应用就无法进行。

2）设置安全策略

在以上三个区域中，用户需要对不同的安全区域设置不同的安全策略。虽然内部网络和 DMZ 区域都属于企业内部网络的一部分，但它们的安全级别（策略）是不同的。对于要保护的大部分内部网络，一般情况下禁止所有来自因特网用户的访问；而由企业内部网络划分出去的 DMZ 区，因需为因特网应用提供相关的服务，所以在一定程度上，

没有内部网络限制那么严格，如 Web 服务器通常允许任何人进行正常的访问。必要时可在防火墙中配置 NAT 对外屏蔽内部网络结构，保护内网安全。

在这种应用环境中，在网络拓扑结构上企事业单位可以有两种选择，这主要是根据企业原有网络设备情况而定。如果企业原来已有边界路由器，则可充分利用原有设备，利用边界路由器的包过滤功能，添加相应的防火墙配置，这样整个网络就相当于有两重防火墙功能。对于需要对外提供服务的公用服务器，则可直接与边界路由器相连，不用经过防火墙。它可只经过包过滤路由器的简单防护，网络结构如图 4-16 所示。在此网络结构中，边界路由器与防火墙一起组成了两道安全防线，并且在这两者之间可以设置一个 DMZ 区，用来放置那些允许外部用户访问的公用服务器设施。

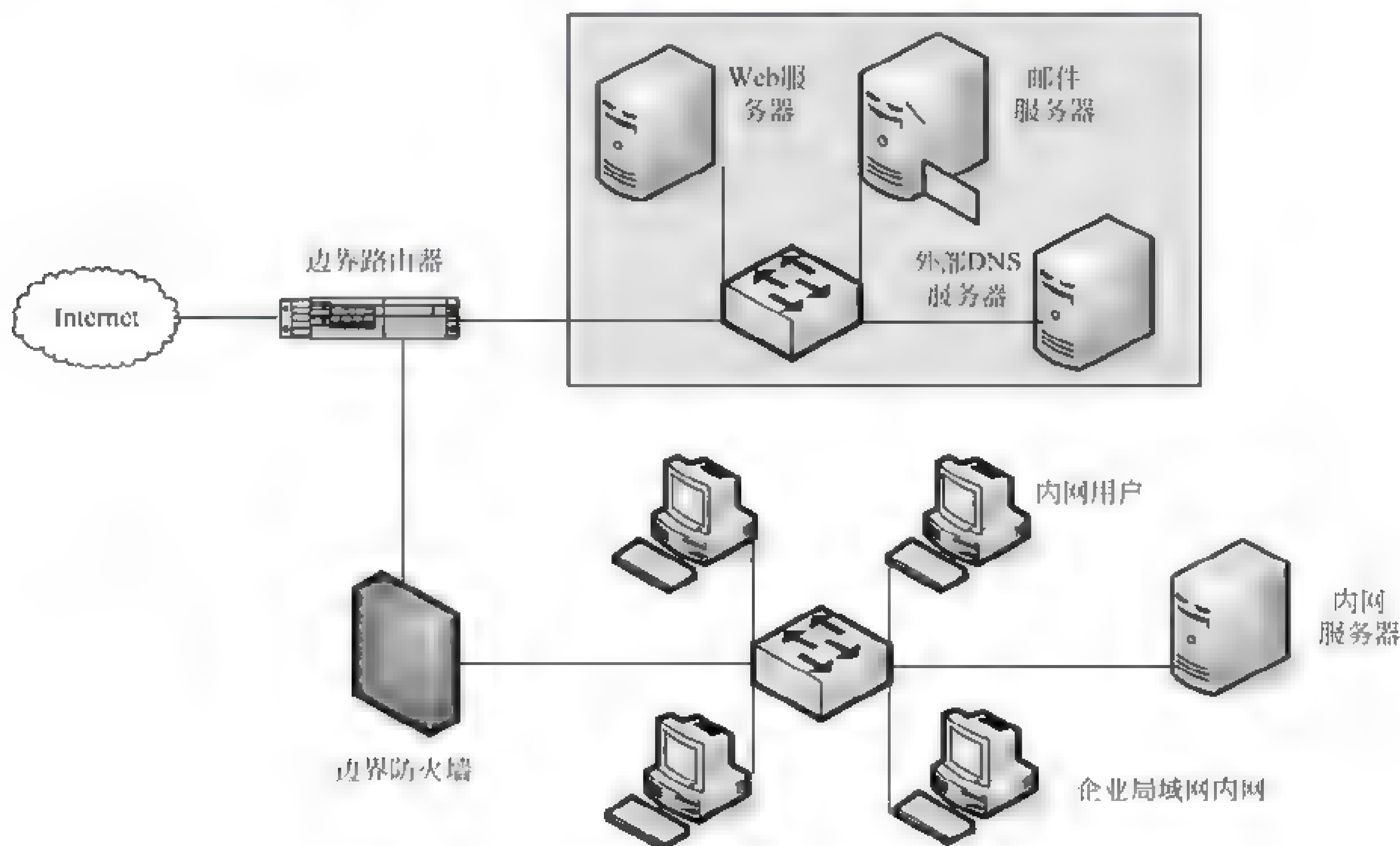


图 4-16　有边界路由器时的网络结构

如果企业原来没有边界路由器，而且也不打算添加边界路由器，则此时仅需由防火墙来保护内部网络。此时，DMZ 区域和需要保护的内部网络连接防火墙的不同 LAN 接口，网络结构如图 4-17 所示，同时设置不同的安全策略。这种拓扑结构虽然只有一道安全防线，但对于大多数中小型企业来说完全可以满足。不过在选购防火墙时要注意，防火墙一定要有两个以上的 LAN 网络接口。

3．控制内部网络不同部门之间的访问

这种应用环境是指在一个企业内部网络之间，对一些安全敏感的部门或者特殊主机进行的隔离保护（当然，所隔离的也可以是一个单独的子网）。通过防火墙保护内部网络中敏感部门的资源不被非法访问。这些所谓的“敏感部门”，通常是指决策部门、财务部门和研究设计部门，其数据对于企业来说非常重要，不能随便被非授权的内网用户访问，

但其工作又不能完全离开企业网络。一种方法是通过配置 VLAN 实现逻辑隔离，另一种有效的方法就是采用防火墙进行隔离。通过防火墙隔离后，尽管同属于一个内部局域网，但是其他用户的访问都需要经过防火墙的过滤，符合条件的用户才能访问。这类防火墙通常不仅通过包过滤来筛选数据包，而且在防火墙中可以设置 ACL（访问控制列表）允许哪些用户可以访问。此外，这种防火墙方案还具有日志记录功能，对网络管理员了解网络安全现状及改进网络非常重要。其网络结构如图 4-18 所示。

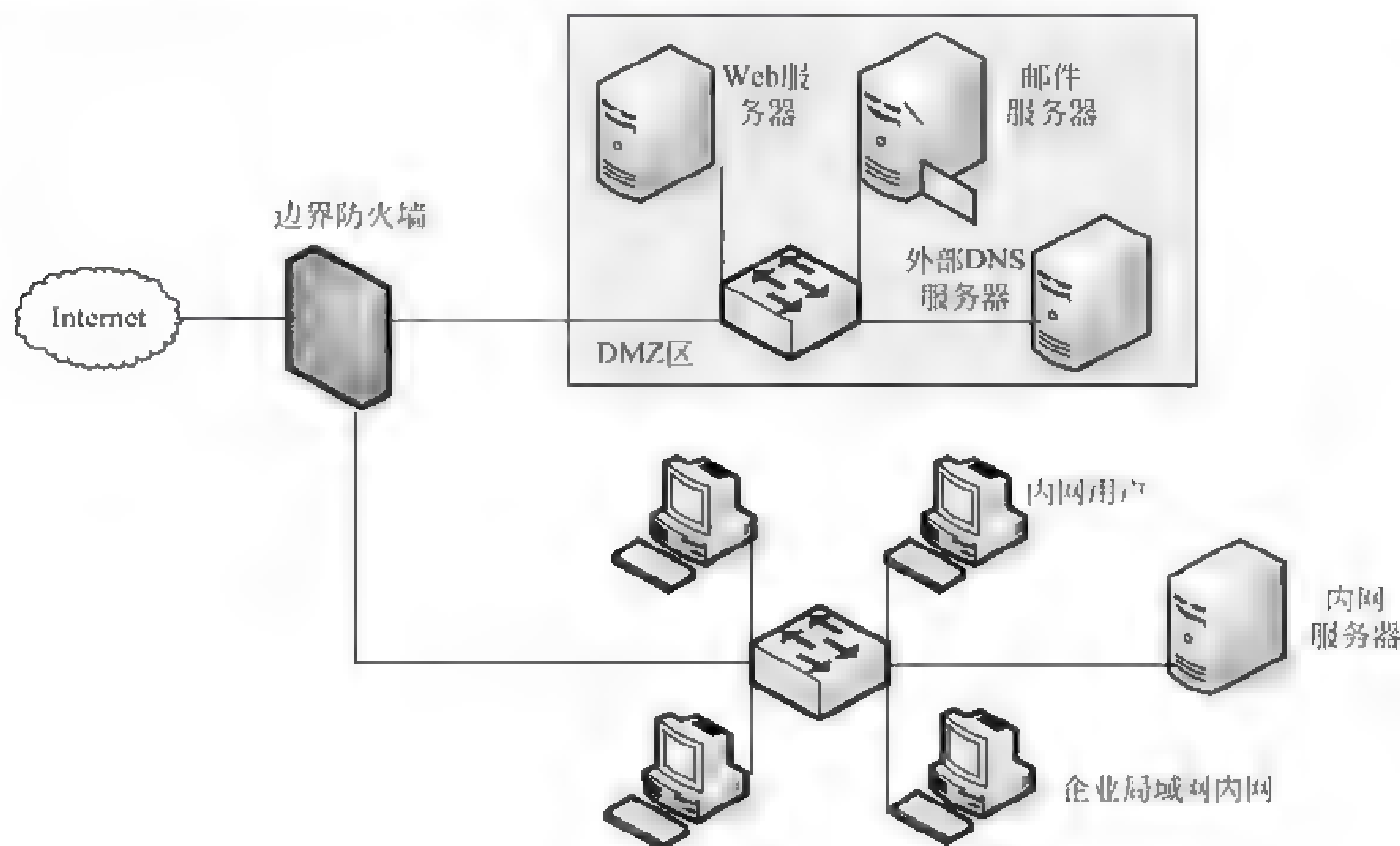


图 4-17 无边界路由器时的网络结构

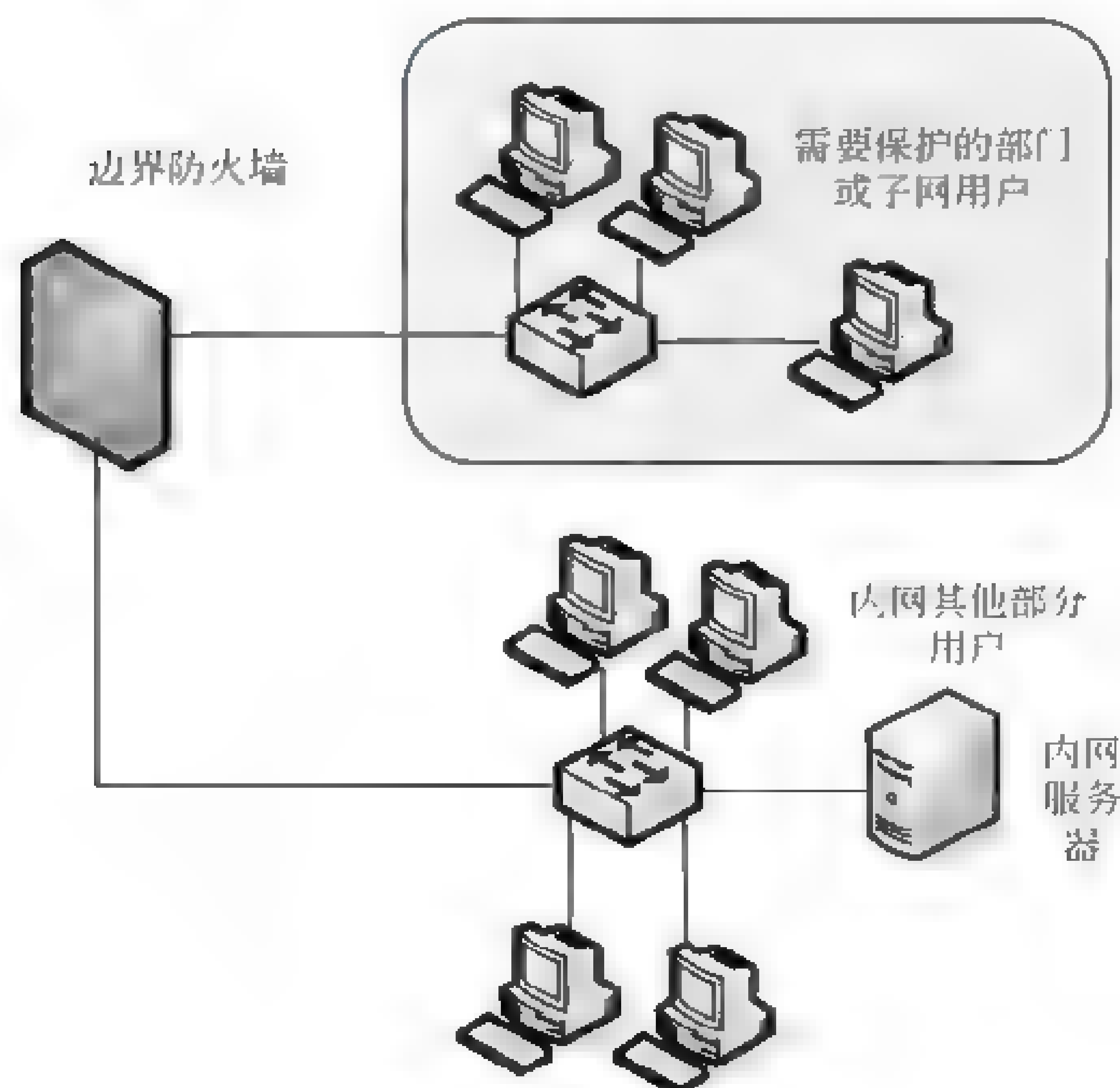


图 4-18 防火墙在内网隔离中的应用

4．控制对服务器中心的网络访问

对于一个服务器中心，如主机托管中心，其众多服务器需要对第三方（合作伙伴、因特网用户等）开放，但是所有这些服务器分别属于不同用户所有，其安全策略也肯定各不相同。如果把它们都定义在同一个安全区域中，显然不能满足各用户的不同需求，这时就要分别设置 DMZ。要按不同安全策略保护这些服务器，可以有两种实施方案。

（1）为每个企业用户的服务器或服务器群单独配置一个独立的防火墙，网络结构如图 4-19 所示。这种方案是一种最直接、最简单的方法，配置方法也最容易，但这种方案从经济上对托管中心来说投资非常大，除非每个企业用户的托管服务器都非常多。另外，托管中心管理员面对这么多防火墙，其管理工作量也相对而言较大。

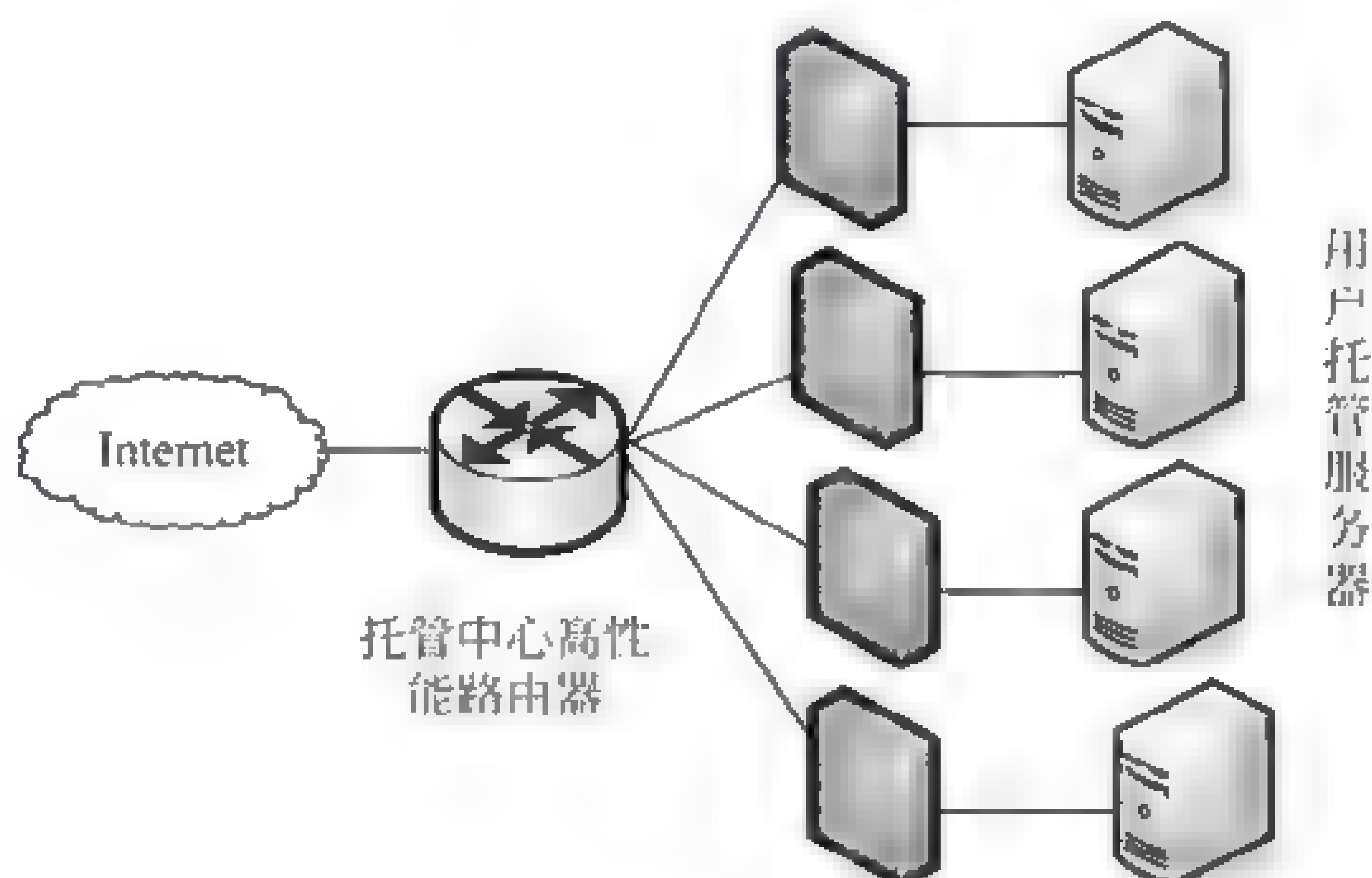


图 4-19　多防火墙方案的网络结构

（2）采用虚拟防火墙方式，网络结构如图 4-20 所示。这主要是利用可网管交换机的 VLAN（虚拟局域网）功能，为每一台连接在交换机上的企业用户服务器群配置成一个单独的 VLAN 子网，然后通过高性能防火墙针对每个 VLAN 子网配置过滤策略和安全规则，就相当于将一个高性能防火墙划分为多个虚拟防火墙。这种方案虽然配置较为复杂，但是比较经济可行。

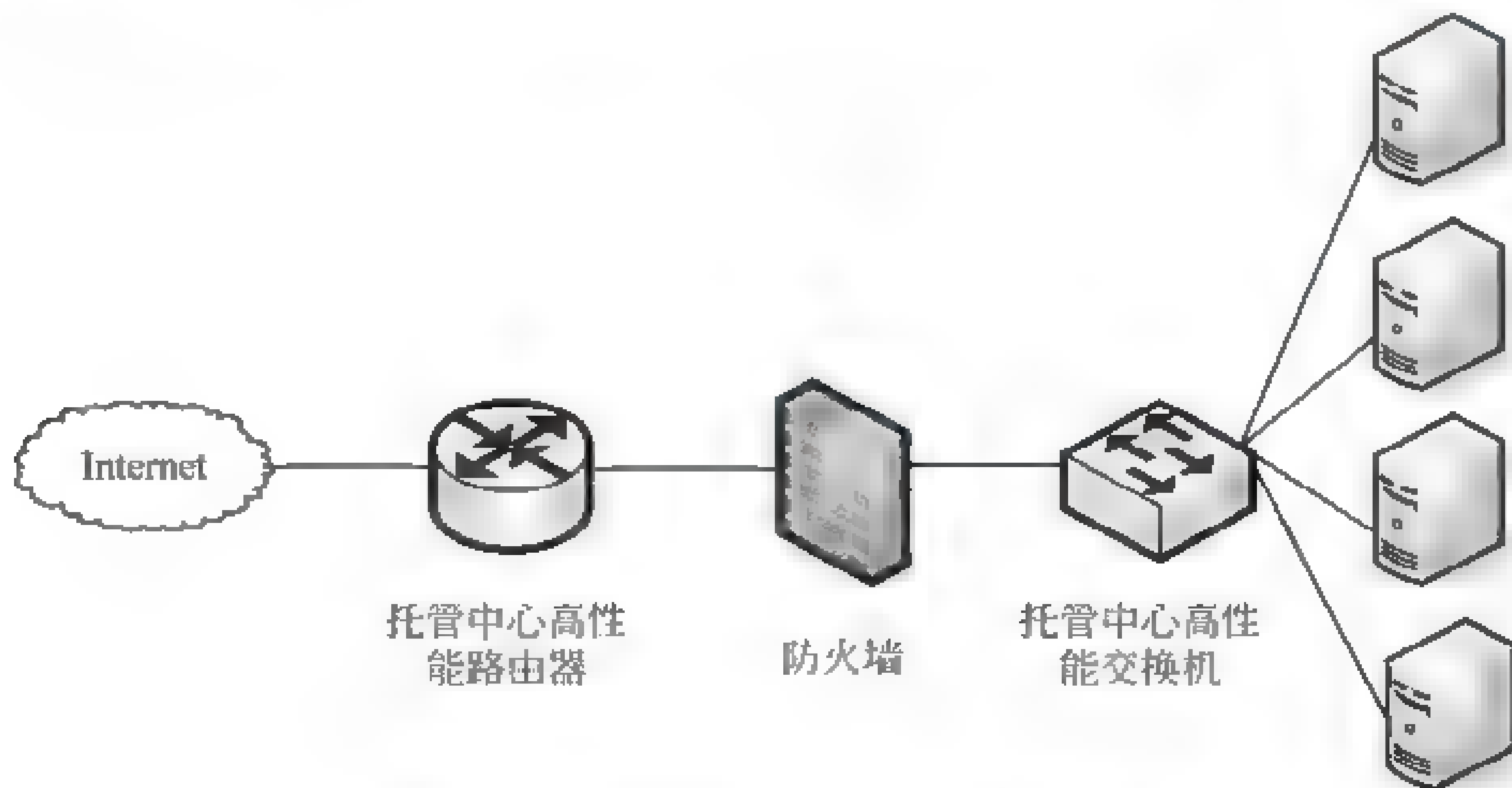


图 4-20　虚拟防火墙方案网络结构

4.3.5 内部防火墙系统应用设计

防火墙一般位于网络边界，所以又俗称边界防火墙。但是现在的网络内部安全形式也不容乐观，于是防火的安全防护职责也就由外向内渗透了，一些防火墙设备开发商就专门针对内网安全控制需求而开发了专用于内网的防火墙产品，使得防火墙的应用更加广泛。

1. 网络上的用户分类

内部防火墙用于控制对内部网络的访问，以及从内部网络进行访问。在部署内部网络防火墙系统时首先要清楚防火墙所要作用的用户类型，有针对性地为各类用户部署策略。总的来说，在这样一个安全防护系统中，从防火墙角度来看，网络上的用户可以分为以下三类。

（1）信任用户。这类用户是指企业的雇员。

（2）部分信任用户。这类用户是指企业的业务合作伙伴，这类用户的信任级别比不受信任的用户高。但是，其信任级别经常比企业的雇员要低。

（3）不信任用户。这类用户是指外部网络用户，如企业公共网站的用户。理论上，来自 Internet 的不受信任的用户应该仅访问外围区域中的 Web 服务器。如果他们需要对内部服务器进行访问，受信任的 Web 服务器会代表他们进行查询，实质上还是不允许不受信任的用户通过此内部防火墙。

2. 防火墙的类别选择及考虑事项

在选择使用的防火墙类别时，应该考虑许多问题。表 4-6 着重说明了这些问题。

表 4-6 内部防火墙类别选择注意事项

考 虑 事 项	实现的防火墙的典型特征
所需的防火墙功能，如安全管理员所指定的	这是所需的安全程度与功能的成本，以及增加安全性可能导致的性能的潜在下降之间的权衡。虽然许多组织希望防火墙提供最高的安全性，但是有些组织并不愿意接受伴随而来的性能降低。例如，对于容量非常大的非电子商务网站，基于通过使用静态数据包筛选器而不是应用程序层筛选获得的较高级别的吞吐量，可能允许较低级别的安全
无论设备是专用的物理设备，提供其他功能，还是物理设备上的逻辑防火墙	这取决于所需的性能、数据的敏感性和需要从外围区域进行访问的频率
设备的管理功能要求，如组织的管理体系结构所指定的	通常使用某种形式的日志，但是通常还需要事件监视机制。可以在这里选择不允许远程管理以阻止恶意用户远程管理设备
吞吐量要求大小很可能由组织内的网络和服务管理员来确定	这些将根据每个环境而变化，但是设备或服务器硬件的功能以及要使用的防火墙功能将确定整个网络的可用吞吐量

续表

考 虑 事 项	实现的防火墙的典型特征
可用性要求	这也要取决于 Web 服务器的访问要求。如果它们主要用于处理提供网页的信息请求，则内部网络的通信量将很低。但是，电子商务环境将需要高级别的可用性

3．内部防火墙规则

内部防火墙监视外围区域和信任的内部区域之间的通信。由于这些网络之间通信类型和数据流的复杂性，内部防火墙的技术要求比外围防火墙的技术要求更加复杂。通常，内部防火墙在默认情况下，或者通过设置将需要遵循以下规则。

（1）默认情况下，阻止所有数据包。

（2）在外围接口上，阻止看起来好像来自内部 IP 地址的传入数据包，以阻止欺骗。

（3）在内部接口上，阻止看起来好像来自外部 IP 地址的传出数据包，以限制内部攻击。

（4）允许从内部 DNS 服务器到 DNS 解析程序 Bastion 主机的基于 UDP 的查询和响应。

（5）允许从 DNS 解析程序 Bastion 主机到内部 DNS 服务器的基于 UDP 的查询和响应。

（6）允许从内部 DNS 服务器到 DNS 解析程序 Bastion 主机的基于 TCP 的查询，包括对这些查询的响应。

（7）允许从 DNS 解析程序 Bastion 主机到内部 DNS 服务器的基于 TCP 的查询，包括对这些查询的响应。

（8）允许 DNS 广告商 Bastion 主机和内部 DNS 服务器主机之间的区域传输。

（9）允许从内部 SMTP 邮件服务器到出站 SMTP Bastion 主机的传出邮件。

（10）允许从入站 SMTP Bastion 主机到内部 SMTP 邮件服务器的传入邮件。

（11）允许来自 VPN 服务器后端的通信到达内部主机并且允许响应返回到 VPN 服务器。

（12）允许验证通信到达内部网络上的 RADIUS 服务器并且允许响应返回到 VPN 服务器。

（13）来自内部客户端的所有出站 Web 访问将通过代理服务器，并且响应将返回客户端。

（14）在外围域和内部域的网段之间支持 Windows Server 2000/2003 域验证通信。

（15）至少支持 5 个网段，在所有加入的网段之间执行数据包的状态检查（线路层防火墙——第 3 层和第 4 层）。

（16）支持高可用性功能，如状态故障转移。

（17）在所有连接的网段之间路由通信，而不使用网络地址转换。

说明：在本部分中提及了“Bastion 主机（堡垒主机）”，其实也就是通常所说的DMZ 区域中的主机。Bastion 主机是位于外围网络中的服务器，向内部和外部用户提供服务。Bastion 主机包括 Web 服务器、E-mail 邮件服务器、FTP 服务器和 VPN 服务器等需要为公众提供服务的服务器。

4．内部防火墙的可用性需求

内部防火墙的应用环境与传统的边界防火墙不太一样，所需的策略规则也不一样，这样对内部防火墙的可用性要求也有所区别。基于硬件的防火墙通常在专用的硬件平台上运行特殊编制的代码，是基于它们可以处理的连接个数和运行的软件的复杂性来衡量的。基于软件的防火墙也可以根据并发连接的数量和防火墙软件的复杂程度进行配置。同时，还应该考虑可能在防火墙服务器上运行的其他软件，如负载平衡和 VPN 软件。此时，可能就需要考虑向上和向外调整防火墙的方法了，如通过添加附加处理器、内存和网卡增加系统的能力，以及使用多系统和负载平衡来分担防火墙任务。目前一些企业级防火墙产品还利用对称多重处理（SMP）来提高性能，就像企业级服务器一样。Windows Server 2003 的网络负载均衡服务可以为一些软件防火墙产品提供容错、高可用性、高效率，但相比硬件的负载平衡方案来说，要逊色不少。

在内部防火墙方案中，根据具体实际需求，可以采用不同的防火墙系统配置方案，如可以是单一无冗余组件的防火墙，也可以是单一有冗余组件的，还可以是合并了某些类型的故障转移和负载平衡机制的容错防火墙集。下面分别介绍这些方案。

1）没有冗余组件的单一防火墙

无冗余组件防火墙是比较普遍的一种防火墙，主要应用于中小型企业。无冗余组件的单一防火墙应用方案如图 4-21 所示。

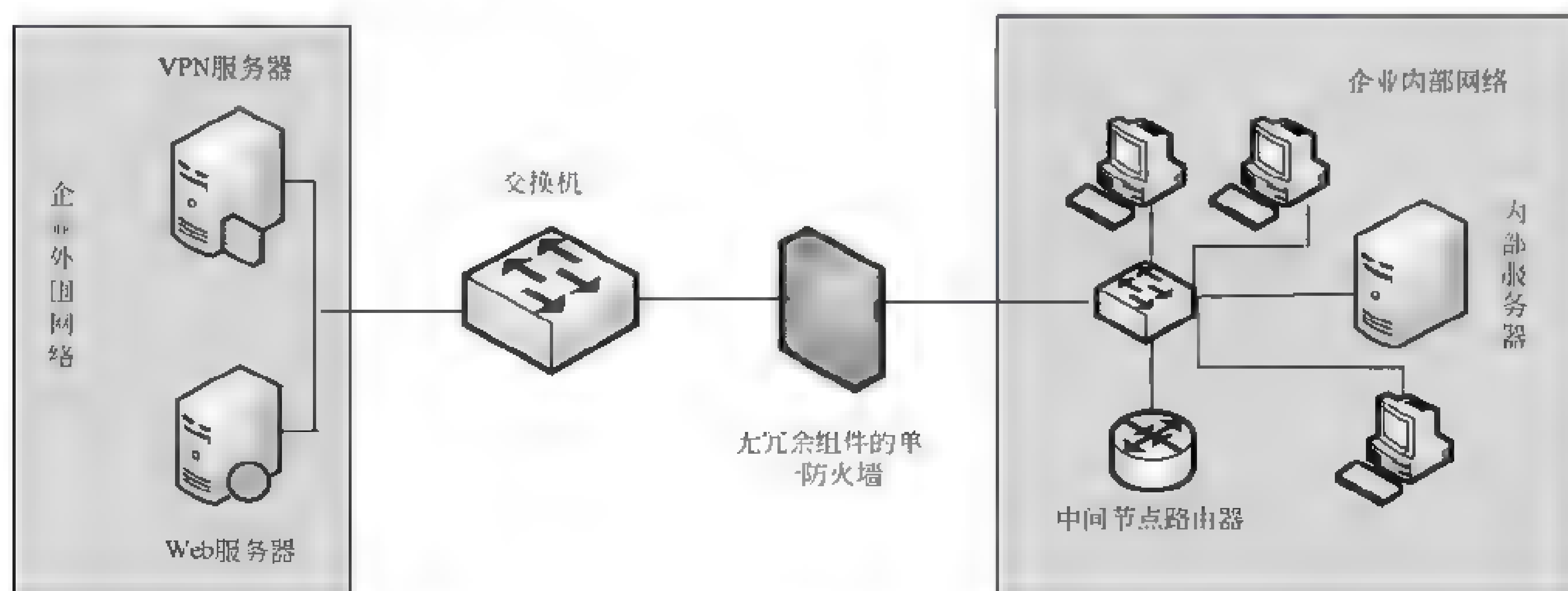


图 4-21 无冗余组件的内部单一防火墙的应用方案

相对于后面即将介绍的有冗余组件防火墙和防火墙冗余对应用方案，单个无冗余组

件的防火墙方案优点主要有以下几个方面。

（1）成本低。由于只有一个防火墙，所以硬件成本和许可成本都较低。

（2）管理简单。管理工作得到简化，因为整个站点或企业只有一个防火墙。

（3）单个记录源。所有通信记录操作都集中在一台设备上，便于管理。

有优点就肯定有缺点，无冗余的单一防火墙的缺点包括以下几个方面。

（1）单一故障点。因为防火墙还用来隔离网络，是内部受保护网络与其他网络的唯一出/入口。对于这样一个单一无冗余的防火墙方案，显然隔离网络之间的出/入口就只是单一的了。这样一来，入站或出站访问存在单一故障点，风险较大。一旦防火墙出现了故障，则整个企业网络都将受到严重影响，特别是对于那些受防火墙保护的网段。

（2）可能的通信瓶颈。原因还是一样，因为单一无冗余防火墙方案中，隔离网络间只存在一个出/入口，这样单一防火墙可能是一个通信瓶颈，当然最终还是取决于连接的个数和所需的吞吐量。所以在选择防火墙时，一定要注意防火墙的吞吐量要与所部署位置的网络流量相适应。

2）具有冗余组件的单一防火墙

具有冗余组件的单一防火墙与前面介绍的无冗余组件单一防火墙相比唯一的区别就是多了一套冗余的组件，具有容错功能，提高了可用性。有冗余组件单一防火墙方案如图 4-22 所示。

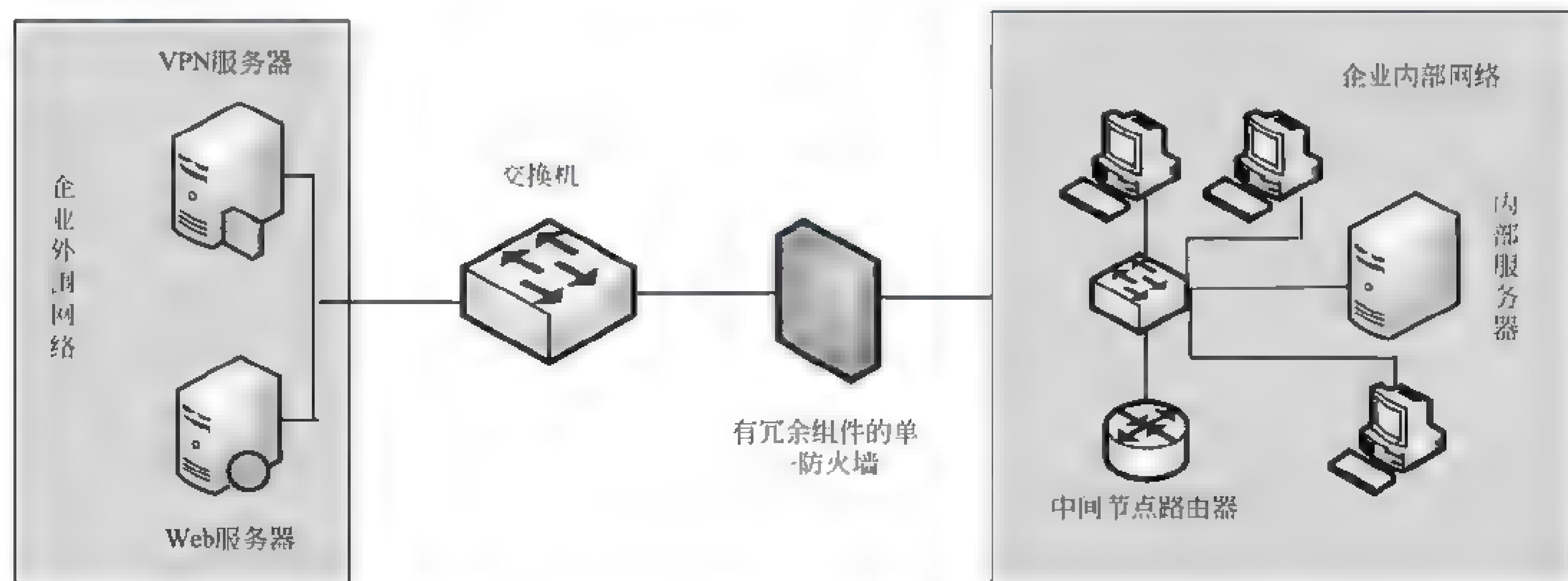


图 4-22　有冗余组件的内部防火墙的应用方案

有冗余组件的单一防火墙具有一些基本的冗余组件，如电源、风扇等，所以相比无冗余组件的防火墙来说，可用性有了一定程度的提高。尽管增加了一些冗余组件，但这类组件的成本也不高。具有冗余组件的单一防火墙方案的缺点与无冗余组件的单一防火墙方案基本一样，在此不再描述。

3）容错防火墙集——防火墙冗余对

容错防火墙集包括一种使每个防火墙成为双工的机制，如图 4-23 所示。

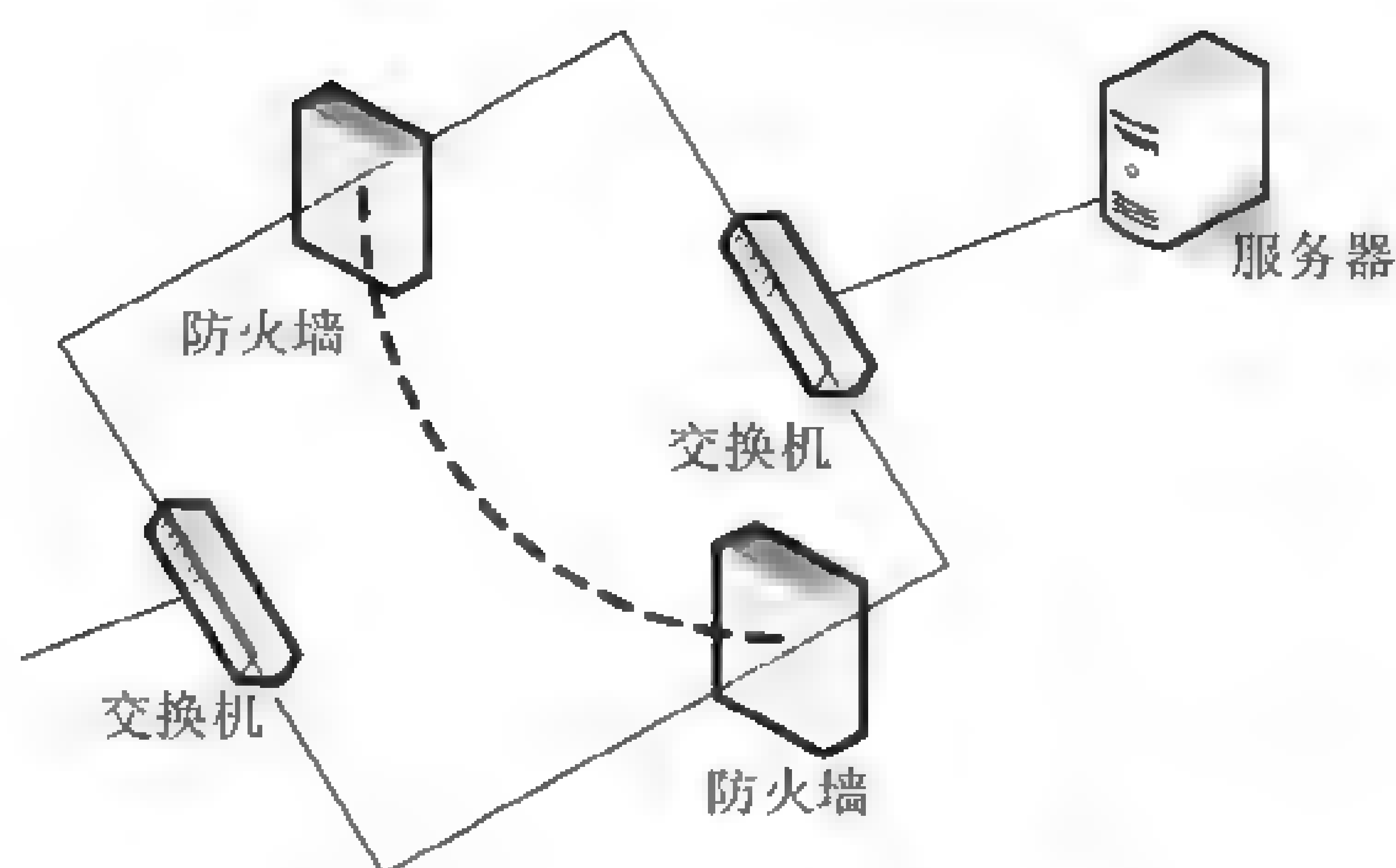


图 4-23 容错防火墙集的应用结构

容错防火墙集的优点主要包括以下几个方面。

（1）容错。使用成对的服务器或者设备有助于提供所需级别的容错能力，使整个防火墙系统的可用性得到极大提高。

（2）集中通信日志。由于两个防火墙或者其中的一个可能正在记录其他合作者或某个单独服务器活动时的通信记录，所以通信日志变得更可靠了。

（3）可能的状态共享。根据产品的不同，集中式的防火墙可能可以共享会话状态。

容错防火墙集在具有以上优点的同时，也带来了一些不足，主要包括以下几个方面。

（1）复杂程度增加。由于网络通信的多路径性质，这一类型的解决方案的网络配置和支持将更复杂，需要比较专业的网络工程师才能胜任。这就要求防火墙提供商能提供全面到位的服务，包括售前/后培训。

（2）配置更复杂。因为同时有两个或两个以上防火墙负责同一部分网络的安全防护，所以必须确保各组防火墙规则的配置都正确，否则可能会导致安全漏洞以及支持问题。

（3）成本增加。当至少需要两个防火墙时，成本将超过单一防火墙集。

5. 内部容错防火墙集配置

在实现内部容错防火墙集（经常称为群集）时，有“主动/被动内部容错防火墙集”和“主动/主动内部容错防火墙集”两种不同配置方法，下面分别予以介绍。

1）主动/被动内部容错防火墙集

在主动/被动内部容错防火墙集中，一个设备（也称为活动节点）将处理所有通信，而另一个设备（被动节点）既不转发通信也不执行筛选，只是保持活动，监视主动节点的状态。这类似于服务器双机容错方案中的“冷备份”方式。

通常，在这种容错方式中，每个节点都传达其可用性和到其伙伴节点的连接状态。此通信经常称为检测信号（服务器容错中称之为“心跳”），每个系统每秒向其他系统发几次检测信号以确保这些连接正在由伙伴节点进行处理。如果被动节点没有接收到来自主动节点的检测信号的时间超过特定的，或者由用户设定的间隔，说明主动节点已经失

败，然后被动节点将承担主动节点的角色。图 4-24 描述了主动/被动内部容错防火墙集工作机制。

主动/被动内部容错防火墙集的优点包括以下几个方面。

（1）配置简单。此配置的设置比后面将要介绍的“主动/主动内部容错防火墙集”方式要简单，因为任何时候只有一个网络路径是活动的。

（2）可预测故障转移负载。因为在故障转移时，整个通信负载将切换到被动节点上，因此需要被动节点管理的通信可以很容易地进行规划。

主动/被动容错防火墙集的缺点则是所有冷备份方式通有的，那就是低利用率，因为在正常工作和不增加吞吐量期间，被动节点对网络不提供任何有用的功能，在投资上是一种浪费。

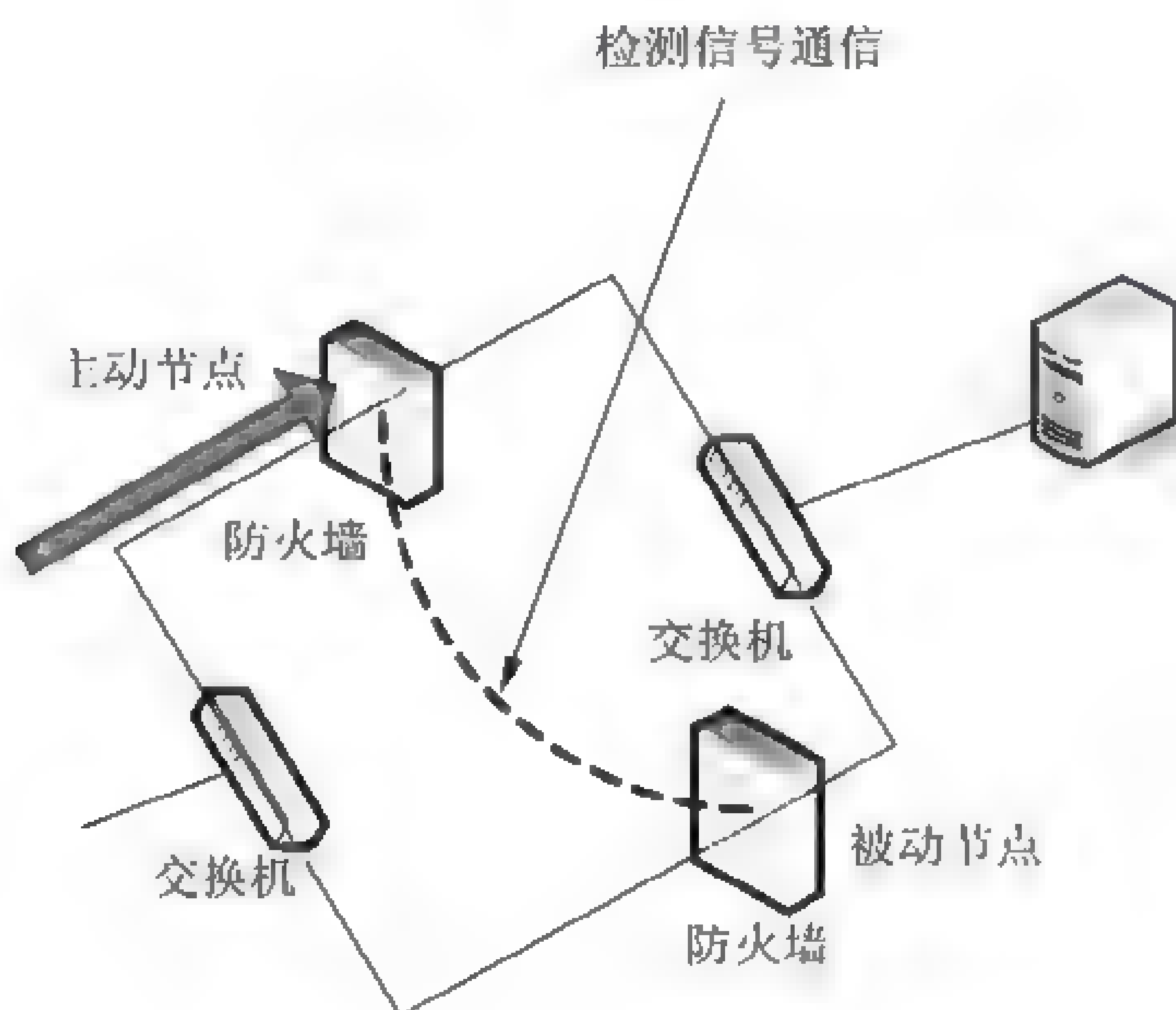


图 4-24　主动/被动内部容错防火墙集的工作机制

2）主动/主动内部容错防火墙集

在主动/主动内部容错防火墙集中，两个或多个节点主动侦听发送到每个节点共享的虚拟 IP 地址的所有请求，与服务器双机容错方案中的“热备份”类似。

在这种容错方式中，负载将通过容错机制唯一使用的算法或者通过基于静态用户的配置在节点之间进行分布。无论使用哪种方法，结果都是每个节点主动地筛选不同的通信。在一个节点失败的事件中，仍存活的节点将分发已失败的节点曾承担的负载的处理。图 4-25 描述了主动/主动容错防火墙集的工作机制。

主动/主动内部容错防火墙集的优点包括以下几个方面。

（1）效率高。由于所有防火墙都向网络提供服务，因此它们的利用率更高。

（2）吞吐量大。在正常操作期间，与“主动/被动内部容错防火墙集”配置相比，此配置可以处理更高级别的通信量，因为所有的防火墙可以同时向网络提供服务。

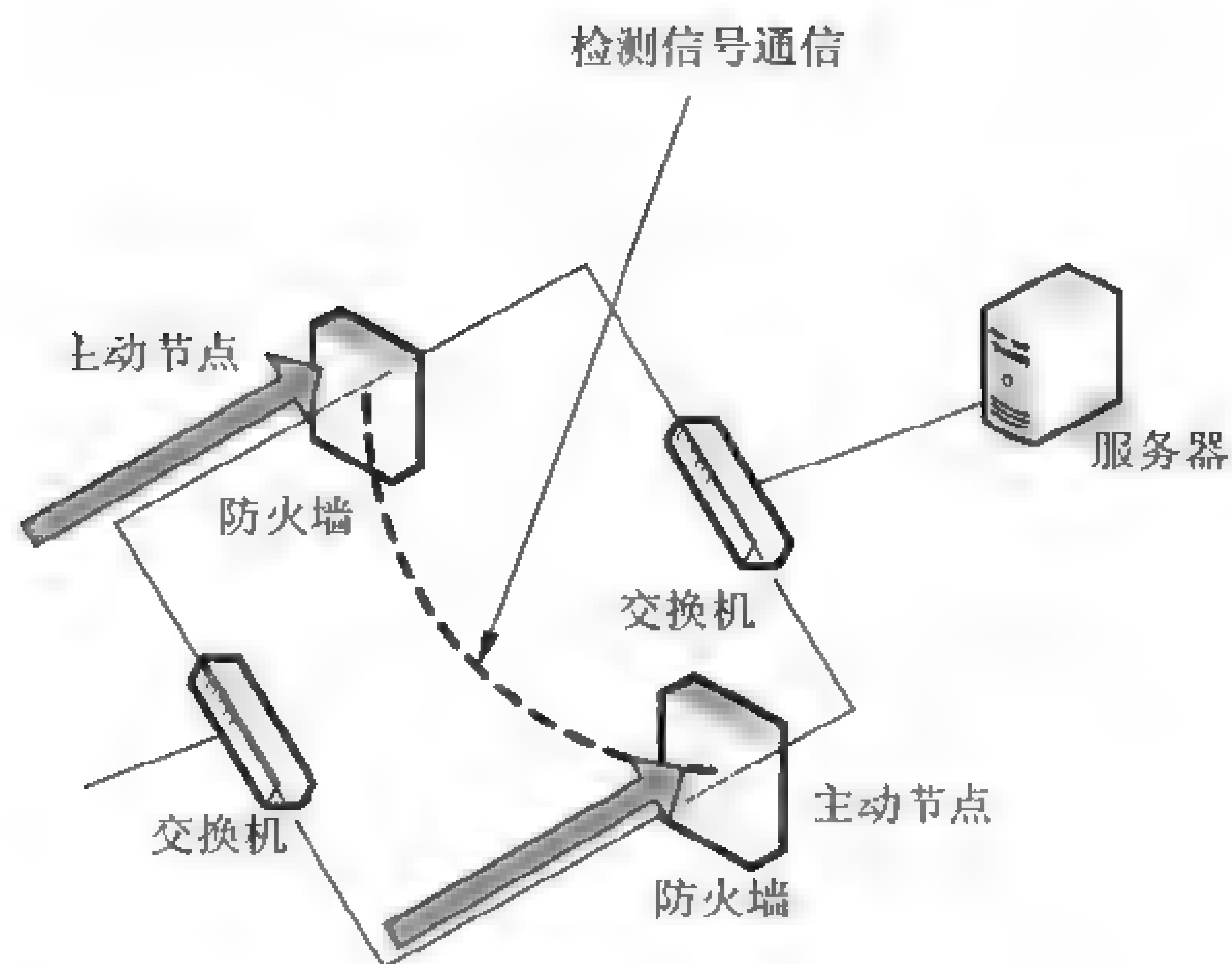


图 4-25 主动/主动内部容错防火墙集的工作机制

主动/主动容错防火墙集的缺点包括以下几个方面。

（1）可能超负荷。如果一个节点发生故障，剩余节点上的硬件资源可能不足以处理整体的吞吐量要求。相应地对此进行规划，了解由于在一个节点失败时，仍存活的节点将承担附加的工作量，由此可能会导致性能下降，这很重要。

（2）复杂程度增加。由于网络通信可以通过多个路由，因此网络配置和故障排除可能更为复杂。

6. 内部防火墙系统设计的其他因素要求

在前面对内部防火墙系统设计的可用性方面的要求作了详细介绍。除此之外，内部防火墙系统设计还需要考虑许多其他因素，如安全性、可伸缩性（也就是通常所说的“可扩展性”）、整合能力和所支持的标准等。下面分别予以介绍。

1）安全性

防火墙产品的安全性极为重要。虽然没有防火墙安全性的行业标准，但是与供应商无关的国际计算机安全协会（ICSA）正在进行一个认证计划，旨在测试已面市的防火墙产品的安全性。ICSA 将对现在市场上可用的大量防火墙产品进行测试。

必须确保防火墙能够达到所需的安全标准，实现此目标的一种方式是选择达到 ICSA 认证的防火墙。此外，应该保持有选择防火墙的跟踪记录。Internet 上有一些安全漏洞数据库，应当尽早查看这些数据库，以获得有关正在考虑购买的产品的漏洞信息。除了确定要购买的产品的漏洞数量和严重程度外，还应评估供应商对已暴露的漏洞的应对措施。

2）可伸缩性

防火墙的可伸缩性主要由所使用的设备的性能特征决定。选择一种调整以满足实际应用的防火墙是明智的。有两种达到可伸缩性的基本方式。

（1）垂直扩展（向上扩展）。所谓“向上扩展”，是指通过增加单一设备的硬件配置数量等手段达到的扩展。无论防火墙是硬件设备还是在服务器上运行的软件解决方案，通过增加内存数量、CPU 处理能力以及网络接口的吞吐量都可以获得各种不同程度的可伸缩性。但是，就可以垂直伸缩的程度来说，每个设备或服务器都有一定的上限。例如，如果购买了一个具有 4 个 CPU 插槽的服务器并且先使用了两个，那么仅可再添加两个 CPU。

（2）水平扩展（向外扩展）。所谓“向外扩展”，是指通过硬件性能提高或者多个不同设备的群集连接等手段实现的扩展。当服务器垂直方向上的扩展到达极限时，则需要进行水平扩展。大多数防火墙（基于硬件的和基于软件的）都可以通过使用某种形式的负载平衡来降低负载。在这种情况下，将多个服务器组成一个群集，对于网络上的客户端来说，它们就像是一个服务器。

增加硬件防火墙容量可能很难。但是，一些硬件防火墙制造商提供了减少负载的解决方案，可以将设备进行堆叠，使之作为单个、负载平衡的单元运行。而一些基于软件的防火墙设计为通过使用多个处理器来增加容量。

多重处理是由基础操作系统控制的，防火墙软件不需要了解附加的处理器，除非防火墙软件可以在多任务方式下操作，否则可能无法实现多个处理器的全部优势。这种方法允许在单一或冗余设备上进行伸缩，通常必须符合在制造时内置的硬件限制。大多数设备类防火墙是按设备可以处理的并发连接的个数来分类的。如果连接要求超过了设备的固定比例的模型可用的连接，硬件设备经常需要进行替换。

如前所述，容错可以内置在防火墙服务器的操作系统中。对于硬件防火墙而言，要实现容错功能则可能要花费额外的成本。

3）整合

合并意味着将防火墙服务合并到另一个设备中，或者将其他服务合并到此防火墙中。合并的好处有以下几个方面。

（1）较低的购买价格。例如，在路由器中通过将防火墙服务合并到另一个服务中，节省了硬件设备的成本，虽然仍然必须购买防火墙软件。同样，如果可以将其他服务合并到防火墙中，就可以节省附加硬件的成本。

（2）减少库存和管理成本。硬件设备数目的减少可以减少操作成本。由于需要较少的硬件升级，布线已经简化，管理变得更简单。

（3）更高的性能。根据所合并的内容，可能会提升性能。例如，将 Web 服务器缓存合并到防火墙中可能会减少附加设备，并且服务将能高速对话而不用通过以太网电缆。

在防火墙系统中，可以采取的合并方式包括以下两种。

（1）将防火墙服务添加到路由器中。大多数路由器可以将防火墙服务合并到其中。此防火墙服务的功能在低成本路由器中可能很简单，但是高端路由器通常具有非常有用的防火墙服务。拥有一个将内部网络中的以太网分段连接在一起的路由器，通过将防火

墙合并到其中，可以节省成本。即使实现了特定的防火墙设备，但是在路由器中实现一些防火墙功能仍然可能有助于限制内部入侵。

（2）将防火墙服务添加到内部交换机中。可以将使用的内部交换机作为一个单元添加到内部防火墙中，从而减少成本并且提高性能。在考虑将其他设备合并到提供防火墙服务的相同服务器或设备中时，必须确保使用给定的服务不会损害防火墙的可用性、安全性或者可管理性。性能方面的考虑也很重要，因为由附加的服务生成的负载将降低防火墙服务的性能。

将服务合并到驻留防火墙服务的相同设备或服务器中的替换方法，是将防火墙硬件设备作为一个单元合并到交换机中。这一方法的成本通常比各种类型的独立防火墙要低，并可以利用交换机的可用性功能，如双电源。这种配置也较容易管理，因为它不涉及单独的设备。此外，使用这种解决方案的系统通常运行较快，因为它使用交换机中的总线，比使用外部线路更快。

4）标准的支持

使用 Internet 协议版本 4（IPv4）的大多数 Internet 协议可以由防火墙来进行保护。这包括较低级别的协议（如 TCP 和 UDP）和较高级别的协议（如 HTTP、SMTP 和 FTP）。应该检查在考虑之中的防火墙产品以确保它支持所需的通信类型。某些防火墙还可以解释 GRE，这是某些 VPN 实现中使用的点对点隧道协议（PPTP）的封装协议。

一些防火墙具有适用于协议如 HTTP、SSL、DNS、FTP、SOCKSv4、RPC、SMTP、H.323 和邮局协议（POP）的内置应用程序层筛选器。即使当前正在使用 IPv4，还应该考虑 TCP/IP 协议和 IPv6 的将来，以及这是否应该是一个对所有防火墙的强制要求。

以上介绍了内部网络防火墙产品的成功选择实际过程。本过程覆盖了防火墙设计的所有方面，包括确定一个解决方案所需的各种评估和分类过程。但事实上没有任何防火墙是百分之百安全的。本节中简要列出的防火墙策略和设计过程只应被看作是整个安全策略的一部分。如果在网络的其他部分中存在弱点，那么强大的防火墙的价值将是有限的。必须将安全策略应用到网络的每个组件中，并且必须为每个组件定义针对环境中固有风险的安全策略。

4.3.6 外围防火墙系统应用设计

本节中介绍的设计准则将从一些主要因素进行考虑（如发展和成本），来帮助用户选择所需的防火墙功能。本节还将介绍一些有关最具破坏性的入侵的信息，以便用户可以确定环境中最有可能发生什么情况，以及确定阻止入侵的方法，这些方法不只是通过安装防火墙，还包括其他一些方法，如加强服务器配置或者与 Internet 服务提供商（ISP）一起就管理问题进行讨论。

来自外部用户和内部用户的网络入侵日益频繁，必须建立保护网络不会受到这些入侵破坏的机制。虽然防火墙可以为网络提供保护，但是它同时会耗费资金，并且会对通

信产生障碍，因此应该尽可能寻找最经济、效率最高的防火墙。设置外围防火墙是为了满足组织边界之外用户的需要。这些用户可能包括以下几种类型。

（1）信任。组织的员工，如各个分支办事处工作人员或者在家工作的用户。

（2）部分信任。组织的业务合作伙伴，这类用户的信任级别比不受信任的用户高。但是，这类用户通常又比组织的员工低一个信任级别。

（3）不信任。例如，组织公共网站的用户。

要考虑的重要一点是，外围防火墙特别容易受到外部攻击，因为入侵者必须破坏该防火墙才能进一步进入网络。因此，它将成为明显的攻击目标。

边界位置中使用的防火墙是通向外部世界的通道。在很多大型组织中，此处实现的防火墙类别通常是高端硬件防火墙或者服务器防火墙，但是某些组织使用的是路由器防火墙。选择某类防火墙用作外围防火墙时，应该考虑一些问题。表 4-7 重点列出了这些问题。

表 4-7　外围防火墙类别选择注意事项

考 虑 事 项	在此位置实现的典型防火墙特征
安全管理员指定的必需防火墙功能	这是一个必需安全性级别与功能成本，以及增加安全性可能导致的性能下降之间的平衡问题。虽然很多组织想通过外围防火墙得到最高的安全性，但有些组织不想影响性能。例如，涉及电子商务的高容量网站，在通过使用静态数据包筛选器而满足使用应用程序层筛选而获取较高级别吞吐量的基础上，可能允许较低级别的安全性
该设备是一个专门的物理设备并提供其他功能，还是物理设备上的一个逻辑防火墙	作为 Internet 和企业网络之间的通道，外围防火墙通常实现为专用的设备，这样是为了在该设备被侵入时将攻击的范围和内部网络的访问性降到最低
组织的管理体系结构决定了设备的可管理性要求	通常，需要使用某些形式的记录，一般还同时需要一种事件监视机制。为了防止恶意用户远程管理该设备，此处可能不允许远程管理，而只允许本地管理
吞吐量要求可能是由组织内部的网络和服务管理员决定的	这些要求会根据每个环境的不同而发生变化，但是设备或者服务器中的硬件处理能力以及所使用的防火墙功能将决定可用的网络整体吞吐量
可用性要求	作为大型组织通往 Internet 的通道，通常需要高级别的可用性，尤其是当外围防火墙用于保护一个产生营业收入的网站时

1．外围防火墙规则

通常情况下，外围防火墙需要以默认的形式或者通过配置来遵循下列规则。

（1）拒绝所有通信，除非显示允许的通信。

（2）阻止声明具有内部或者外围网络源地址的外来数据包。

（3）阻止声明具有外部源 IP 地址的外出数据包（通信应该只源自堡垒主机）。

（4）允许从 DNS 解析程序到 Internet 上的 DNS 服务器的基于 UDP 的 DNS 查询和应答。

（5）允许从 Internet DNS 服务器到 DNS 解析程序的基于 UDP 的 DNS 查询和应答。

（6）允许基于 UDP 的外部客户端查询 DNS 解析程序并提供应答。

（7）允许从 Internet DNS 服务器到 DNS 解析程序的基于 TCP 的 DNS 查询和应答。

（8）允许从出站 SMTP 堡垒主机到 Internet 的外出邮件。

（9）允许外来邮件从 Internet 到达入站 SMTP 堡垒主机。

（10）允许从代理发起的通信从代理服务器到达 Internet。

（11）允许代理应答从 Internet 定向到外围的代理服务器。

2．外围防火墙系统的可用性要求

要增加外围防火墙的可用性，可以将其实现为带有冗余组件的单个防火墙设备，或者实现为外围容错防火墙集，其中结合一些类型的故障转移和负载平衡机制。这些选项的优点和缺点在下面的内容中讲述。

（1）单个无冗余组件外围防火墙。单个无冗余组件的外围防火墙网络结构如图 4-26 所示。单个无冗余组件外围防火墙的优点和缺点与 4.3.5 节介绍的单个无冗余组件内部防火墙相似，在此不再赘述。

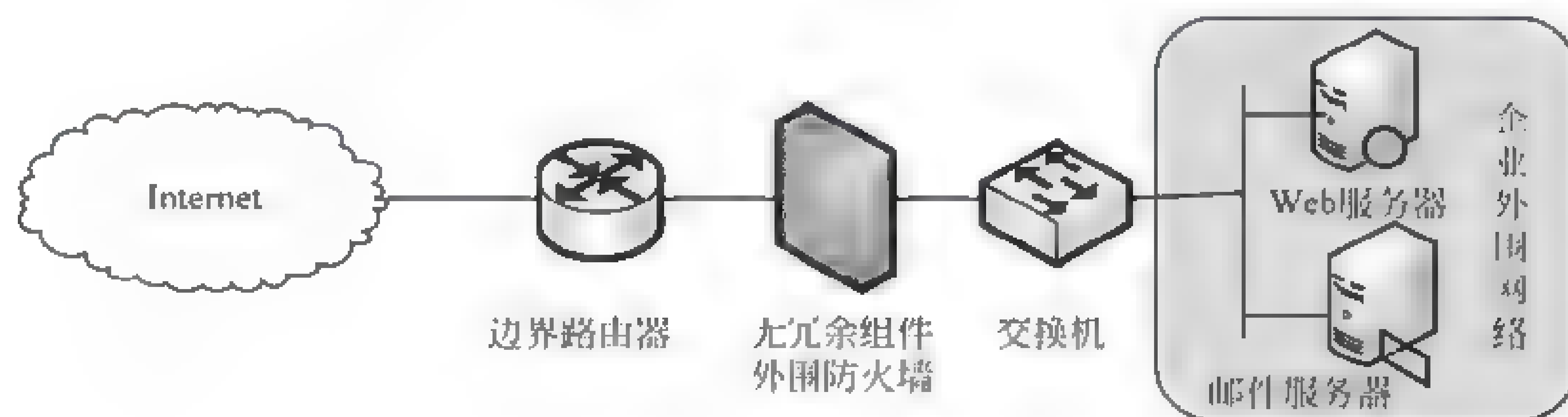


图 4-26 单个无冗余组件的外围防火墙应用结构

（2）单个带冗余组件外围防火墙。单个带冗余组件的外围防火墙应用结构如图 4-27 所示。单个带冗余组件外围防火墙的优点和缺点也与 4.3.5 节介绍的单个带冗余组件内部防火墙相似，不再赘述。

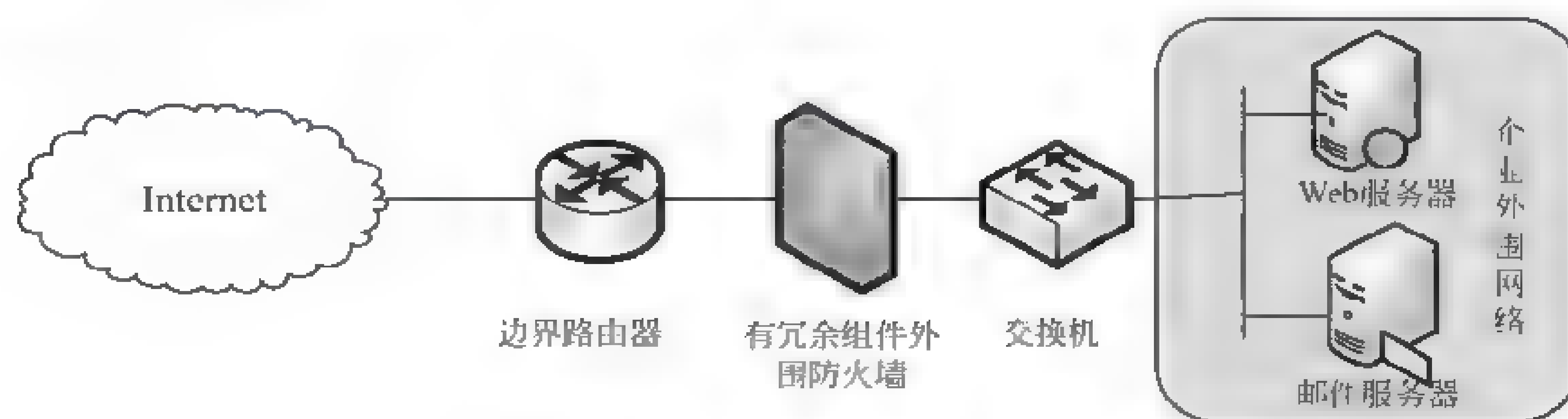


图 4-27 单个带冗余组件的外围防火墙应用结构

（3）外围容错防火墙集。外围容错防火墙集包括为每个防火墙配置备用装置的机制，如图 4-28 所示。

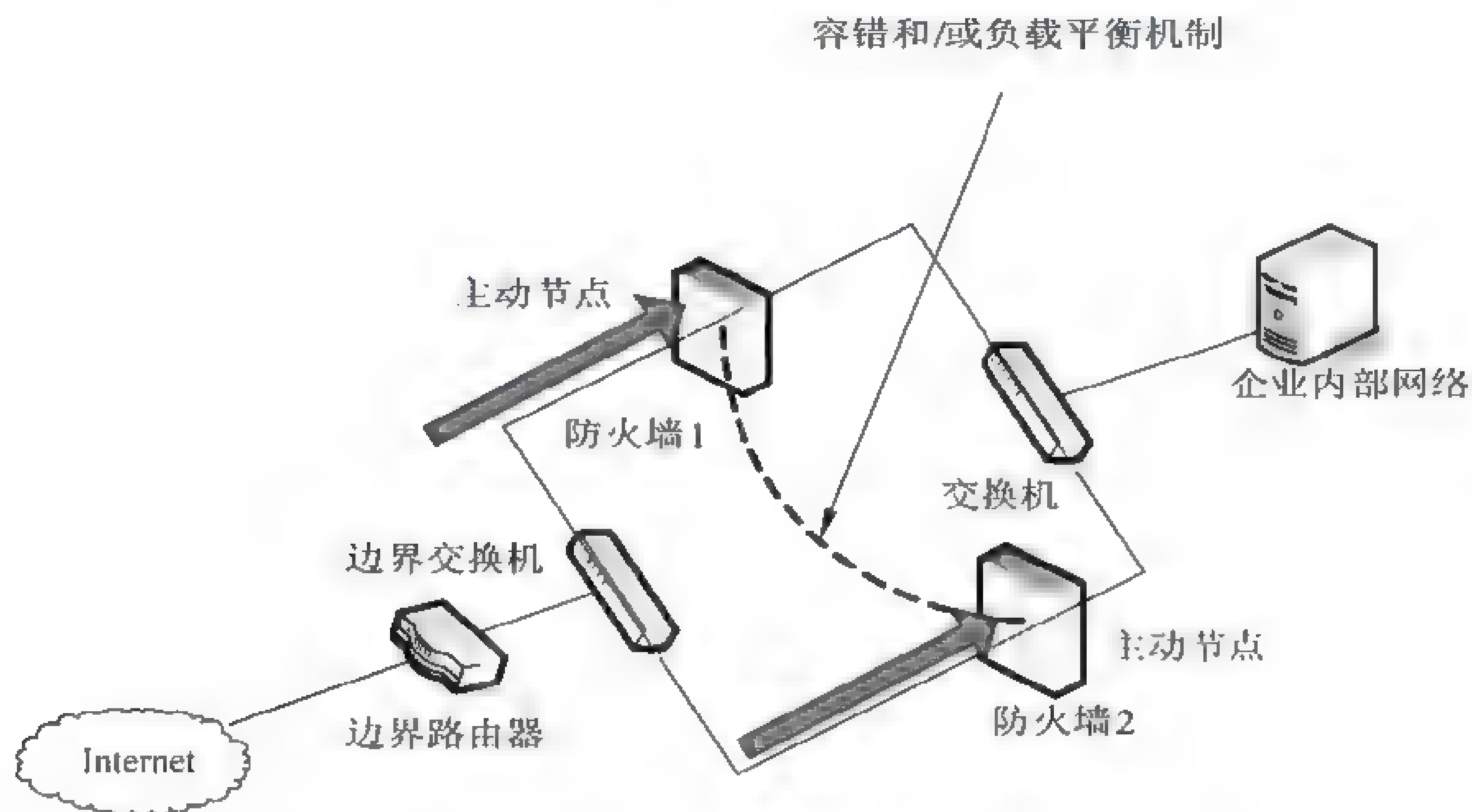


图 4-28　外围容错防火墙集应用结构

外围容错防火墙集的优点和缺点也与 4.3.5 节介绍的内部容错防火墙集的优、缺点相似，不再赘述。有关两种不同的容错方案配置也与内部容错防火墙集类似，不再赘述，至于外围防火墙系统设计的其他方面要求参见 4.3.5 节的内容即可。

4.3.7　防火墙与 DoS/DDoS 攻击

DoS/DDoS 攻击是一种非常有效的进攻方式，能够利用大量的服务请求来占用过多的服务资源，从而使合法用户无法得到正常服务。常见的 DoS/DDoS 攻击可以分为两大类：一类是针对系统或协议漏洞的攻击，如 Ping of Death、TearDrop 等，例如 Teardrop 是基于 UDP 的病态分片数据包的攻击方法。其工作原理是向被攻击者发送多个分片的 IP 包（IP 分片数据包中包括该分片数据包属于哪个数据包以及在数据包中的位置等信息），某些操作系统收到含有重叠偏移的伪造分片数据包时将会出现系统崩溃、重启等现象。Teardrop 攻击利用 UDP 包重组时重叠偏移（假设数据包中第二片 IP 包的偏移量小于第一片结束的位移，而且算上第二片 IP 包的 Data，也未超过第一片的尾部，这就是重叠现象）的漏洞对系统主机发动拒绝服务攻击，最终导致系统宕机。对于 Windows 系统会导致蓝屏死机，并显示 STOP 0x0000000A 错误。另一类攻击是消耗计算机或网络中匮乏的、有限的资源，如占用大量网络带宽。这类攻击比较典型的如 UDP flood、SYN flood 和 ICMP flood 等，SYN Flood 攻击以多个随机的源主机地址向目的主机发送 SYN 包，而在收到目的主机的 SYN ACK 后并不回应，这样，目的主机就为这些源主机建立了大

量的连接队列，而且由于没有收到 ACK 一直维护着这些队列，造成了系统资源的大量消耗而不能向正常请求提供服务。

1．防火墙抵御 DoS/DDoS 攻击原理

从现在和未来看，防火墙都是抵御 DoS/DDoS 攻击的重要组成部分，这是由防火墙在网络拓扑的位置和扮演的角色决定的。下面以港湾网络有限公司基于 NP（Net Processor，网络处理器）架构开发的 SmartHammer 系列防火墙为例说明其在各种网络环境中对 DoS/DDoS 攻击的有效防范。

1）基于状态的资源控制，保护防火墙资源

港湾网络 SmartHammer 防火墙支持 IP Inspect 功能，防火墙会对进入防火墙的资料做严格的检查，各种针对系统漏洞的攻击包如 Ping of Death、TearDrop 等，会自动被系统过滤掉，从而保护了网络免受来自于外部的漏洞攻击。对防火墙产品来说，资源是十分宝贵的，当受到外来的 DDoS 攻击时，系统内部的资源全都被攻击流所占用，此时正常的资料报文肯定会受到影响。SmartHammer 基于状态的资源控制会自动监视网络内所有的连接状态，当有连接长时间未得到应答就会处于半连接的状态，浪费系统资源，当系统内的半连接超过正常的范围时，就有可能是遭受到了攻击。SmartHammer 防火墙基于状态的资源控制能有效防止此类情况，其采用的方法主要包括以下几种。

（1）控制连接、与半连的超时时间，必要时，可以缩短半连接的超时时间，加速半连接的老化。

（2）限制系统各个协议的最大连接值，保证协议的连接总数不超过系统限制，在达到连接上限后删除新建的连接。

（3）限制系统符合条件源/目的主机连接数量。

（4）针对源或目的 IP 地址进行 IP 流量控制，SmartHammer 防火墙 IP Inspect 模块可以限制每个 IP 地址使用的资源，用户在资源控制的范围内时，使用并不会受到任何影响，但当用户感染蠕虫病毒或发送攻击报文等情况时，针对流的资源控制可以限制每个 IP 地址发起的连接数目，超过限制的连接将被丢弃。这种做法可以有效抑制病毒产生攻击的效果，避免其他正常使用的用户受到影响。

（5）设置协议流门限值。单位时间内如果穿过防火墙的“同类”数据流超过门限值后，可以设定对该种类的数据流进行阻断，这对于防止 IP、ICMP 和 UDP 等非连接的 Flooding 攻击具有很好的防御效果。

2）智能 TCP 代理有效防范 SYN Flood

SYN Flood 是 DDoS 攻击中危害性最强，也是最难防范的一种。这种攻击利用 TCP 协议缺陷，发送大量伪造的 TCP 连接请求，从而使得被攻击方资源耗尽（CPU 满负荷或内存不足）。SmartHammer 系列防火墙能够利用智能 TCP 代理技术，判断连接合法性，保护网络资源。

防火墙工作时，并不会立即开启 TCP 代理（以免影响速度），只有当网络中的 TCP

半连接达到系统设置的 TCP 代理启动警戒线时，正常 TCP Intercept 会自动启动，并且当系统的 TCP 半连接超过系统 TCP Intercept 高警戒线时，系统进入入侵模式，此时新连接会覆盖旧的 TCP 连接。此后，系统全连接数增多，半连接数减少，当半连接数降到入侵模式低警戒线时，系统退出入侵模式。如果此时攻击停止，系统半连接数量逐渐降到 TCP 代理启动警戒线以下，智能 TCP 代理模块停止工作。通过智能 TCP 代理可以有效防止 SYN Flood 攻击，保证网络资源安全。

3）利用 Netflow 对 DoS 攻击和病毒进行监测

网络监控在抵御 DDoS 攻击中有重要的意义。SmartHammer 防火墙支持 NetFlow 协议，它将网络中的数据包以流的方式进行记录，并封装为 UDP 包发送到 NetFlow 分析器上，这样就为网络管理、流量分析和监控、入侵检测等提供了丰富的资料来源。SmartHammer 防火墙可以在不影响转发性能的同时记录、发送 NetFlow 信息。网络管理员通过在防火墙相关接口下开启 NetFlow 采集功能，并设置 NetFlow 输出服务器地址，就可以利用一些网络安全管理平台对接收到的资料进行分析、处理。

（1）利用 NetFlow 监视网络流量。防火墙可以有效地抵御 DDoS 攻击，但当攻击流数量超过一定程度，已经完全占据网络带宽时，虽然防火墙已经通过安全策略把攻击数据包丢弃，但由于攻击数据包已经占据了所有的网络带宽，正常的用户访问依然无法完成。此时网络的流量是很大的，SmartHammer 防火墙可以利用内置的 NetFlow 统计分析功能，查找攻击流的数据源，并上报上级 ISP，对数据流分流或导入黑洞路由。此外，当发现网络流量异常时，可以利用 Netflow 功能有效地查找、定位 DDoS 攻击的来源。

（2）利用 NetFlow 监视蠕虫病毒。防止蠕虫病毒的攻击，重要的是防止蠕虫病毒的扩散，只有尽早发现，才可以迅速采取措施有效阻止病毒。各种蠕虫病毒在感染了系统后，为了传播自身，会主动向外发送特定的数据包并扫描相关端口。利用这个特性，网络管理员在安全管理平台上通过对 NetFlow 采集的数据流进行分析，就可以知道哪些主机感染了病毒，然后采取相应的措施。

值得指出的是，防火墙在网络拓扑中的位置对抵御攻击也有很大影响，通常盒式防火墙被设计放置在网络的出口，这种情况下，虽然防火墙能够抵御从外部产生的攻击，但一旦网络内部的 PC 通过浏览网页、收发 E-mail、下载等方式感染蠕虫病毒或有人从内部发起恶意攻击时，防火墙是没有防护能力的。

港湾网络的 SmartHammer ESP-FW 防火墙模块可以解决此类问题，ESP-FW 是港湾网络 BigHammer6800 系列交换机的一个安全模块，它继承了 SmartHammer 盒式防火墙的相关安全特性内置于交换机中，有效抵御来自内部网络的攻击。在插入了防火墙模块后，交换机可以选择将相关 VLAN 加入防火墙中，受防火墙保护。以 VLAN 作为保护对象的另一大优点是利于网络扩展，当有一个新增部门出现时，不需要再增加投资就可以使新增部门得到保护，网络部署异常灵活。这样，当内部网络中出现异常数据流时，防火墙可以有效限制该数据的转发，保护其他 VLAN 不受影响。

2. 防火墙抵御 DoS/DDoS 攻击配置示例

下面以港湾的 SmartHammer 防火墙为例，说明如何通过配置资源控制保护内部网络或特定主机免受 DoS/DDoS 攻击。

1）资源控制的配置

```
ip inspect max 500000                       //系统总的连接数
ip inspect max 500000 tcp                   //系统总的 TCP 连接数
ip inspect max 100000 udp                   //系统总的 UDP 连接数
ip inspect maxincomplete high 20000 tcp     //TCP 半连接最高水位线
ip inspect maxincomplete low 10000 tcp      //TCP 半连接最低水位线
ip inspect one-minute high 20000 tcp        //TCP 每分钟半连接最高水位线
ip inspect one-minute low 10000 tcp         //TCP 每分钟半连接最低水位线
ip inspect idletime 3600 tcp                //TCP 全连接超时时间
```

当 TCP 半连接达到最高水位线时，防火墙开始清除超过的半连接，一直清到最低水位线为止。TCP 每分钟半连接也是一样的处理机制。

2）限制主机的最大连接数

网络中经常会出现一些病毒，感染的主机会自动向变换地址的目标主机发送 TCP 连接请求或 ICMP 报文，如以前爆发的冲击波及其变种就具有类似的特征，通过限制网络内主机的最大连接数目可以有效地达到防范效果。

```
access-list 40 permit 192.168.0.0 255.255.0.0 //定义访问列表 40 的地址范围
ip inspect max flow 50 src list 40
//限制符合条件的主机最多建立 50 个连接，超过这个数目，新的连接报文将被丢弃
```

3）适应特殊主机的需求

网络内部可能会存在一些特殊连接需求的主机，如内部的 DNS 服务器或一些部门的代理服务器等，对于这些主机它们的连接请求数一般会超过一般主机，所以需要对这些特殊的主机执行特殊的流限制。

对于不十分了解网络内主机构成的管理员来说，不断地通过 show ip inspect statistics flow 查看网络内主机建立连接的情况是一种比较好的方式，通过恰当地定义网络主机的连接数量，可以很大程度地防止一些网络病毒的攻击或 DoS 攻击。

```
access-list 11 permit host 10.1.0.4
access-list 12 permit host 10.1.1.1
access-list 13 permit 10.0.0.0 255.0.0.0
ip inspect max flow 1000 src list 11 //设置主机 10.1.0.4 的最大连接为 1000
ip inspect max flow 10000 src list 12  //设置主机 10.1.1.1 的最大连接为 10000
ip inspect max flow 50 src list 13
//设置 10.0.0.0/8 网络中其他主机的最大连接为 50
```

4）对服务器资源的保护

通过 IP Inspect 对目的主机的保护，主要用于对内部主机保护的情况。如果需要保护 DMZ 区域的服务器资源，则可以采用以下配置。

```
access-list 2001 permit tcp any 10.1.0.4 eq 21
access-list 2001 permit tcp any 10.1.0.5 eq http
ip inspect max flow 500 dst list 2001
ip inspect max flow 1000 dst-dport list 2001
```

3．使用防火墙防御 SYN Flood 攻击

使用防火墙是防御 SYN Flood 攻击的最有效方法之一。但是我们常见的硬件防火墙有多种，到底哪种才具有此种防御功能呢?又该如何配置防火墙呢?下面先来了解包过滤型和应用代理型防火墙防御 SYN Flood 攻击的原理。

1）两种主要类型防火墙的防御原理

应用代理型防火墙的防御方法是在客户端要与服务器建立 TCP 连接的三次握手过程中，因为它位于客户端与服务器端（通常分别位于外、内部网络）中间，充当代理角色，这样客户端要与服务器端建立一个 TCP 连接，就必须先与防火墙进行三次 TCP 握手，当客户端和防火墙三次握手成功之后，再由防火墙与客户端进行三次 TCP 握手，完成后再进行一个 TCP 连接的三次握手。一个成功的 TCP 连接所经历的两个三次握手过程，先是客户端到防火墙的三次握手，再是防火墙到服务器端的三次握手。

从整个过程可以看出，由于所有的报文都是通过防火墙转发，而且未同防火墙建立起 TCP 连接就无法同服务器端建立连接，所以使用这种防火墙就相当于起到一种隔离保护作用，安全性较高。当外界对内部网络中的服务器端进行 SYN Flood 攻击时，实际上遭受攻击的不是服务器而是防火墙。而防火墙自身则又是具有抗攻击能力的，可以通过规则设置，拒绝外部客户端不断发送的 SYN 报文。

但是，采用这种防火墙有个很大的缺点，那就是客户端和服务器端建立一个 TCP 连接时，防火墙就进行 6 次握手，可见防火墙的工作量是非常大的。因此，采用这种防火墙要求该防火墙要有较高的处理速度及较大内存。应用代理型防火墙通常不适合应用于访问流量大的服务器或者网络。

包过滤型防火墙工作于 IP 层或者 IP 层之下，对于外来的数据报文，它只是起一个过滤的作用。当数据包合法时，它就直接将其转发给服务器，起到的是转发作用。在包过滤型防火墙中，客户端同服务器的三次握手直接进行，并不需要通过防火墙来代理进行。包过滤型防火墙的效率要较网关型防火墙高，适用于数据流量大的场景。但是这种防火墙如果配置不当，会让攻击者绕过防火墙而直接攻击到服务器。而且允许数据量大会更有利于 SYN Flood 攻击。这种防火墙适合于大流量的服务器，但是需要设置妥当才能保证服务器具有较高的安全性和稳定性。

2）防御 SYN Flood 攻击的防火墙设置

除了可以直接采用以上两种不同类型的防火墙进行 SYN Flood 防御外，还可进行一些特殊的防火墙设置来达到目的。针对 SYN Flood 攻击，防火墙通常有三种防护方式：SYN 网关、被动式 SYN 网关和 SYN 中继。

（1）SYN 网关。在这种方式中，防火墙收到客户端的 SYN 包时，直接转发给服务器；防火墙收到服务器的 SYN/ACK 包后，一方面将 SYN/ACK 包转发给客户端，另一方面以客户端的名义给服务器回送一个 ACK 包，完成一个完整的 TCP 三次握手，让服务器端由半连接状态进入连接状态。当客户端真正的 ACK 包到达时，有数据则转发给服务器，否则丢弃该包。由于服务器在连接状态要比半连接状态使用更少的资源，所以这种方法能有效地减轻对服务器的攻击。

（2）被动式 SYN 网关。在这种方式中，设置防火墙的 SYN 请求超时参数，让它小于服务器的超时期限。防火墙负责转发客户端发往服务器的 SYN 包，包括服务器发往客户端的 SYN/ACK 包和客户端发往服务器的 ACK 包。这样，如果客户端在防火墙计时器到期时还没发送 ACK 包，防火墙将往服务器发送 RST 包，以使服务器从队列中删除该半连接。由于防火墙的超时参数小于服务器的超时期限，因此这样也能有效防止 SYN Flood 攻击。

（3）SYN 中继。在这种方式中，防火墙在收到客户端的 SYN 包后，并不向服务器转发而是记录该状态信息，然后主动给客户端回送 SYN/ACK 包。如果收到客户端的 ACK 包，表明是正常访问，由防火墙向服务器发送 SYN 包并完成三次握手。这样，由防火墙作为代理来实现客户端和服务器端的连接，可以完全过滤恶意连接发往服务器。

4.3.8　防火墙应用实例

1．PIX 防火墙

思科系统公司（Cisco Systems，Inc.）成立于 1984 年 12 月，是全球领先的因特网解决方案提供者。Cisco Secure PIX 防火墙系列是业界领先的产品之一，具有很好的安全性、可靠性，特别是以突出的性能而著称。

下面以 PIX Firewall 525 为例介绍 PIX Firewall 的基本配置方法。

在进行配置之前，首先需要了解 PIX 防火墙提供的 4 种管理访问模式。

（1）非特权模式：PIX 防火墙开机自检后，就是处于这种模式，系统提示符为 pixfirewall>。

（2）特权模式：输入 enable 进入特权模式，可以改变当前配置，系统提示符为 pixfirewall#。

（3）配置模式：输入 configure terminal 进入此模式，绝大部分的系统配置都在这里进行，系统提示符为 pixfirewall（config）#。

（4）监视模式：PIX 防火墙在开机或重启过程中，按住 Escape 键或发送一个 Break

字符，进入监视模式，可以更新操作系统映像和口令恢复，系统提示符为 monitor>。

在配置 PIX 防火墙时，有 6 个基本命令是必须的：nameif、interface、ip address、nat、global 和 route。

1）配置防火墙接口的名字，并指定安全级别（nameif）

```
Pix525(config)#nameif ethernet0 outside security0
Pix525(config)#nameif ethernet1 inside security100
Pix525(config)#nameif dmz security50
```

在默认配置中，以太网 0 被命名为外部接口（outside），安全级别是 0；以太网 1 被命名为内部接口（inside），安全级别是 100。其他接口安全级别取值范围为 1～99，数字越大安全级别越高。若添加新的接口，可以输入命令：

```
Pix525(config)#nameif pix/intf3 security40(安全级别任取)
```

2）配置以太网接口参数（interface）

```
Pix525(config)#interface ethernet0 auto
```

auto 选项表明接口为系统自适应网卡类型。

```
Pix525(config)#interface ethernet1 100full
```

100full 选项表示接口以 100Mbps 以太网全双工通信方式工作。

```
Pix525(config)#interface ethernet1 100full shutdown
```

shutdown 选项表示关闭这个接口，若启用接口去掉 shutdown。

3）配置内外网卡的 IP 地址（ip address）

```
Pix525(config)#ip address outside 202.114.38.42 255.255.255.0
Pix525(config)#ip address inside 192.168.101.1 255.255.255.0
```

上述例子中，PIX 525 防火墙在外网的 IP 地址是 202.114.38.42，内网 IP 地址是 192.168.101.1。

4）指定要进行转换的内部地址（NAT）

网络地址翻译（NAT）的作用是将内网的私有 IP 转换为外网的公有 IP。NAT 命令总是与 global 命令一起使用，这是因为 NAT 命令可以指定一台主机或一段范围的主机访问外网，访问外网时需要利用 global 所指定的地址池进行对外访问。

nat 命令语法：

```
nat(if_name)nat_id local_ip [netmark]
```

其中，(if name）表示内网接口名字，如 inside；nat id 用来标识全局地址池，使它

与其相应的 global 命令相匹配；local ip 表示内网被分配的 IP 地址，例如，0.0.0.0 表示内网所有主机可以对外访问；[netmark]表示内网 IP 地址的子网掩码。

```
Pix525(config)#nat(inside)1 0 0
```

表示启用 nat，内网的所有主机都可以访问外网，用 0 可以代表 0.0.0.0。

```
Pix525(config)#nat(inside)1 172.16.5.0 255.255.0.0
```

表示只有 172.16.5.0 这个网段内的主机可以访问外网。

5）指定外部地址范围（global）

global 命令把内网的 IP 地址翻译成外网的 IP 地址或一段地址范围。

global 命令语法：

```
global(if_name)nat_id ip_address-ip_address [netmark global_mask]
```

其中，（if_name）表示外网接口名字，如 outside；nat_id 用来标识全局地址池，使它与其相应的 nat 命令相匹配；ip_address-ip_address 表示翻译后的单个 IP 地址或一段 IP 地址范围；[netmark global_mask]表示全局 IP 地址的网络掩码。

```
Pix525(config)#global(outside)1 202.114.38.43-202.114.38.52
```

表示内网的主机通过 PIX 防火墙要访问外网时，PIX 防火墙将使用 202.114.38.43-202.114.38.52 这段 IP 地址池为要访问外网的主机分配一个全局 IP 地址。

```
Pix525(config)#global(outside)1 202.114.38.43
```

表示内网要访问外网时，PIX 防火墙将为访问外网的所有主机统一使用 202.114.38.43 这个单一 IP 地址。

```
Pix525(config)#no global(outside)1 202.114.38.43
```

表示删除这个全局表项。

6）设置指向内网和外网的静态路由（route）

route 命令配置语法：

```
route(if_name)ip netmask gateway_ip [metric]
```

其中，（if_name）表示接口名字，如 inside、outside；ip、netmask 分别代表 IP 地址和子网掩码；gateway_ip 表示网关路由器的 ip 地址；[metric]表示到 gateway_ip 的跳数，通常默认是 1。

```
Pix525(config)#route outside 0 0 202.114.38.1 1
```

表示一条指向边界路由器（ip 地址 202.114.38.1）的默认路由。

```
Pix525(config)#route inside 10.1.1.0 255.255.255.0 192.168.101.2 1
Pix525(config)#route inside 10.2.0.0 255.255.0.0 192.168.101.2 1
```

如果内部网络只有一个网段，设置一条默认路由即可；如果内部存在多个网络，需要配置一条以上的静态路由。

7）配置 fixup 协议

fixup 命令的作用是启用、禁止、改变一个服务或协议通过 PIX 防火墙，由 fixup 命令指定的端口是 PIX 防火墙要侦听的服务，请参见下面的例子。

```
Pix525(config)#fixup protocol ftp 21  启用 ftp 协议,并指定 ftp 的端口号为 21
Pix525(config)#fixup protocol http 80
Pix525(config)#fixup protocol http 1080 为 http 协议指定 80 和 1080 两个端口
Pix525(config)#no fixup protocol smtp 25 禁用 smtp 协议
```

以上介绍的只是 Cisco PIX　Firewall 的基本配置命令，要更好地利用防火墙进行网络安全管理，还需要对 PIX 防火墙进行高级配置。由于篇幅有限，高级配置方法在此不作介绍，用户可参照 PIX　Firewall 用户手册。

2．天网防火墙

天网个人防火墙是早期国内用户比较喜欢的一款个人防火墙软件。天网个人防火墙提供多种预先设置的安全级别，同时也支持用户自定义应用程序的安全规则与系统的安全策略，支持应用程序通信控制，同时具备自动识别功能，但绝大部分的应用程序无法自动识别，用户需要在程序第一次访问网络时配置防火墙规则。此外，它还提供特洛伊木马和入侵检测功能，可以通过厂商的安全数据库自动查找系统的漏洞。

天网防火墙个人版是个人计算机使用的网络安全程序，根据管理者设定的安全规则把守网络，提供强大的访问控制、信息过滤等功能，帮助用户抵挡网络入侵和攻击，防止信息泄露。天网防火墙把网络分为本地网和因特网，可针对来自不同网络的信息设置不同的安全方案，适合于任何方式上网的用户。

1）安全级别设置

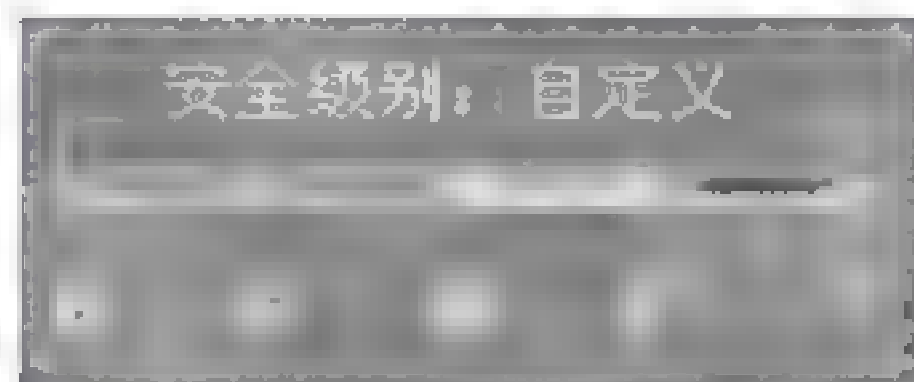


图 4-29　天网个人防火墙的默认安全级别

天网个人版防火墙的默认安全级别分为低、中、高、扩 4 个等级（如图 4-29 所示），默认的安全等级为中级。用户可以根据自己的需要调整自己的安全级别，方便实用。对

于普通的个人上网用户，建议使用中级安全规则，它可以在不影响使用网络的情况下，最大限度地保护机器不受到网络攻击；对于需要频繁试用各种新的网络软件和服务、又需要对木马程序进行足够限制的用户，建议其使用扩展级安全规则，可以对各种木马及间谍程序有相当的限制并保留一定的网络访问便利。

值得注意的是，天网的简易安全级别是为了方便不熟悉天网使用的用户能够很好地使用天网而设的。正因为如此，如果用户选择了采用简易的安全级别设置，那么天网就会屏蔽高级的“IP 规则设定”里规则的作用。

2）IP 规则设置

IP 规则是针对整个系统的网络层数据包监控而设置的。利用自定义 IP 规则，用户可针对个人不同的网络状态，设置自己的 IP 安全规则，使防御手段更周到、更实用。用户可以按“自定义 IP 规则”键或者在“安全级别”中单击按钮进入 IP 规则设置界面。

IP 规则设置的操作界面如图 4-30 所示。

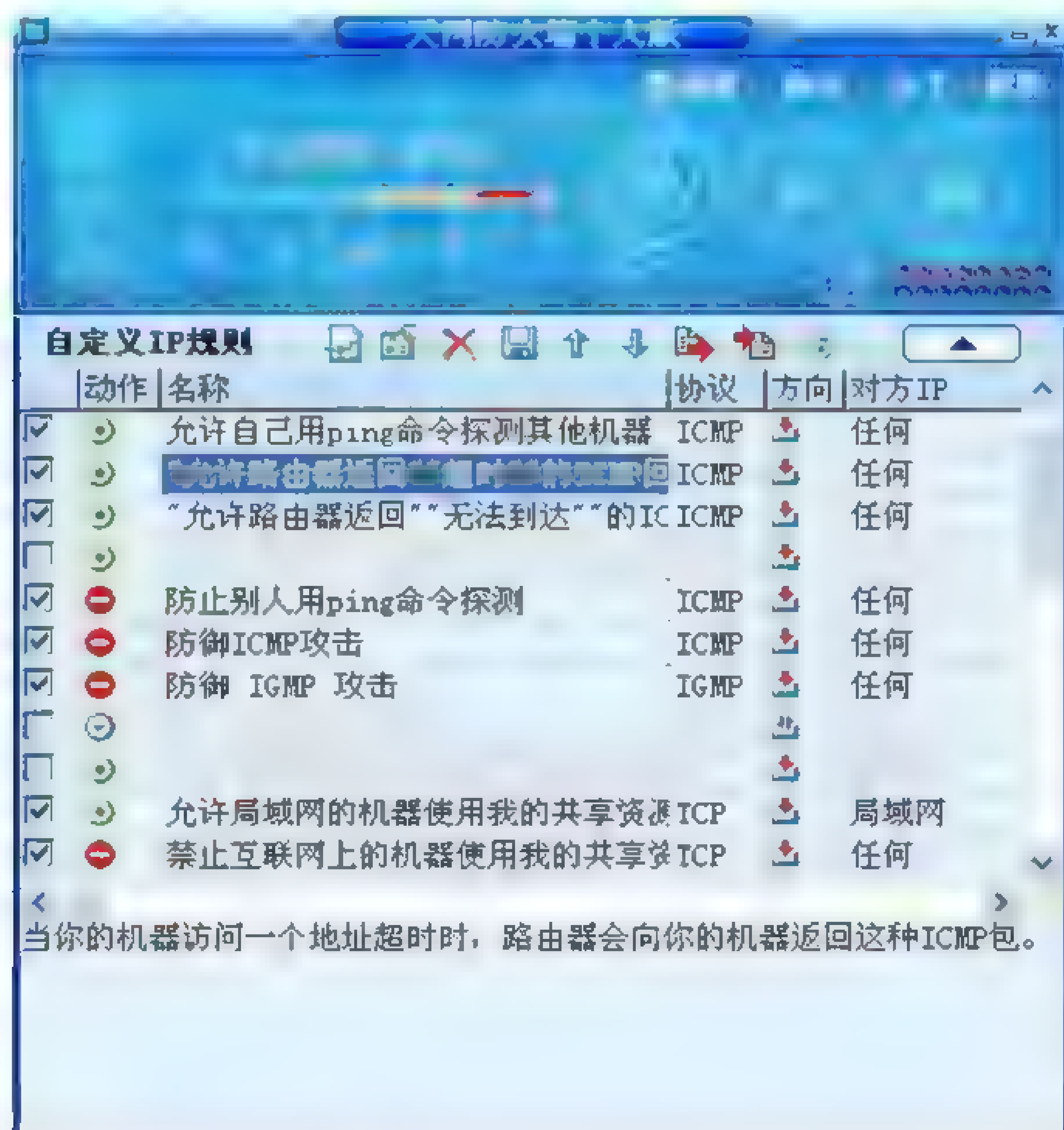


图 4-30 自定义 IP 规则

实际上，天网防火墙个人版本身已经默认设置了相当好的默认规则，一般用户并不需要做任何 IP 规则修改，就可以直接使用。但是对于一些高级用户而言，天网防火墙自

身提供的一些默认规则可能不能满足要求，此时用户可以自行定义和添加新的 IP 规则。

假如当前用户想要禁止接收任何 SNMP 的报文，可以通过图 4-31 所示的操作实现。

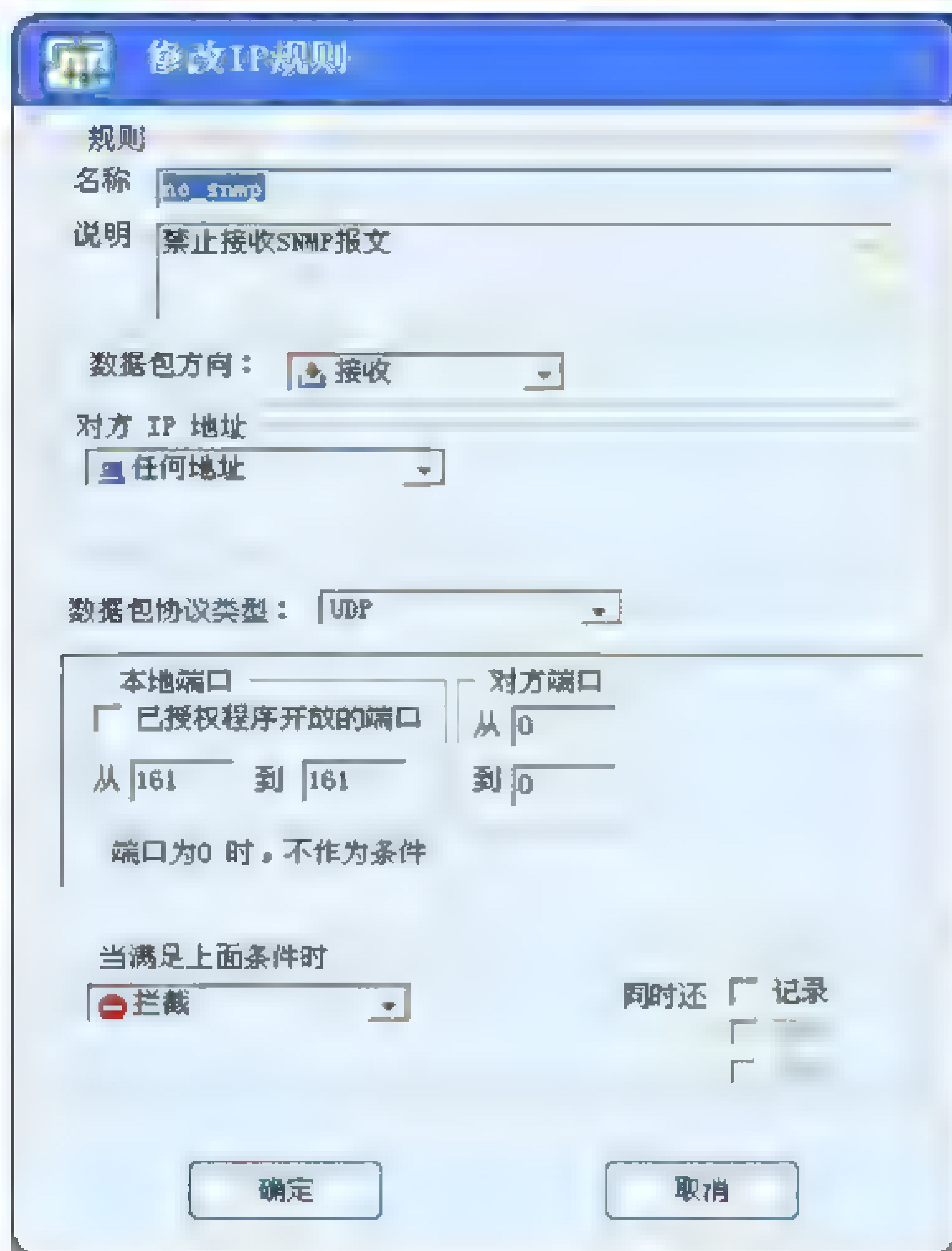


图 4-31　添加和修改 IP 规则

（1）单击“自定义 IP 规则”工具栏中的“增加规则”按钮（第一个按钮），将弹出一个用于定义增加 IP 规则的对话框。

（2）在“规则”选项区域中的“名称”文本框和“说明”列表框中任意填写自定义规则的名称以及相关的描述，便于查找和阅读。

（3）“数据包方向”选择“接收”，表示该规则是针对进入的还是发出的数据包有效。

（4）“对方 IP 地址”选项区域用于确定选择数据包从哪里来或是去哪里，其中“任何地址”表示数据包从任何地方来都适合本规则，“局域网网络地址”是指数据包来自和发往局域网，“指定地址”可以自己输入一个特定的地址，“指定的网络地址”可以输入一个网络号和掩码。

（5）由于 SNMP 是基于 UDP 协议的，因此“数据包协议类型”选择 UDP。

（6）由于 SNMP 在本地机器上使用的是 UDP 161 端口，因此在“本地端口”中填写的端口号为 161。

（7）在“当满足上面条件时”选项区域的下拉列表框中选择“拦截”，表示让指定的数据包无法进入当前用户的机器。

（8）单击“确定”按钮，将指定的规则添加到 IP 规则列表中去。

应用程序规则管理与 IP 规则设置的操作类似，限于篇幅原因，在此就不再赘述，用户可以自行参看相关的帮助文档和使用手册。

4.4 ISA Server 应用配置

ISA Server（Internet Security and Acceleration Server）是微软公司提供的著名路由级网络防火墙。微软公司分别在 2004 年 7 月 13 日和 2006 年 7 月 31 日正式发布了 Microsoft ISA Server 2004 和 Microsoft ISA Server 2006 和 ISA Server 2004 相比，ISA Server 2006 作了如下更新和升级。

（1）所有包含在 ISA Server 2004 SP2 中的新增特性，如 BITS 缓存、HTTP 压缩支持、基于 DiffServ 协议的 HTTP 优先级等。

（2）增强了对 OWA 发布和多个 Web 站点发布的支持，并新增了对 SharePoint Portal Server 发布的支持。

（3）新增了单点登录特性，支持针对通过某个 Web 侦听器所发布的所有 Web 服务的单点登录。

（4）新增了服务器场功能，支持通过多个 Web 服务器组成服务器群集以实现负载均衡，并且此特性无需 Windows 的 NLB 或群集支持。

（5）强化了 DDoS 防御功能，极大地增强了对于 DDoS 攻击的防范能力。

4.4.1 ISA Server 的安装

1. 安装准备

（1）网络：在安装 ISA Server 服务器以前，应保证网络正常工作，这样可以避免一些未知的问题。本节中使用的网络环境如图 4-32 所示。

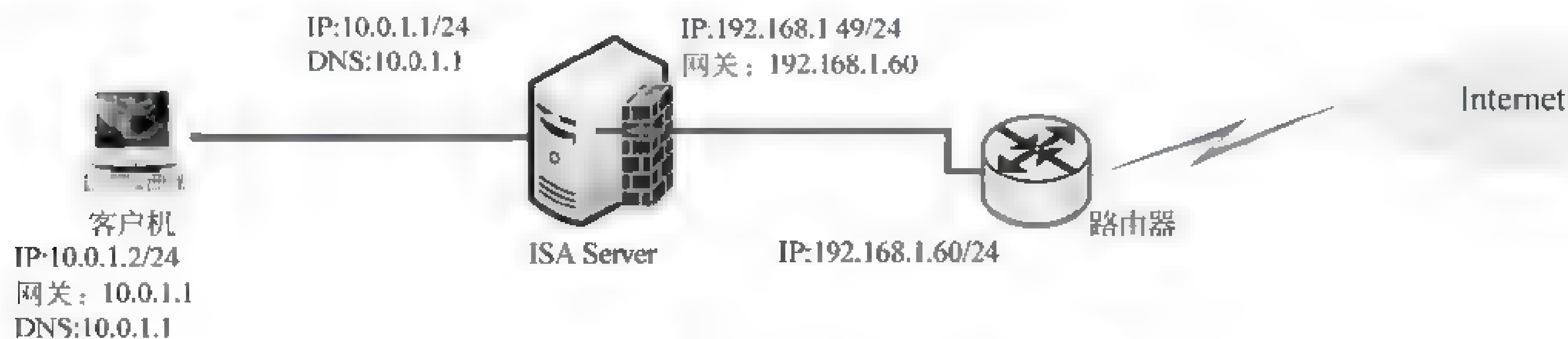


图 4-32 ISA Server 应用环境

（2）网络适配器：必须为连接到 ISA Server 服务器的每个网络单独准备一个网络适

配器，至少需要一个网络适配器。但是，在单网络适配器计算机上安装的 ISA Server 服务器通常是为发布的服务器提供一层额外的应用程序筛选保护或者缓存来自 Internet 的内容使用。

（3）DNS 服务器：ISA Server 服务器不具备转发 DNS 请求的功能，必须使用额外的 DNS 服务器。或者在内部网络中建立一个 DNS 服务器，或者使用外网（Internet）的 DNS 服务器。

2．安装 ISA Server

假定在 ISA Server 服务器上已经建立好了一个内部的 DNS 服务器；所有客户端以 ISA Server 机的内部接口（10.0.1.1）作为它的网关和 DNS 服务器。由于在设计的时候考虑了很多人性化特性和管理特性，ISA Server 使用起来非常简单。当然，这一切都是以正确的安装为基础的。运行 ISA Server 安装光盘根目录下的 ISAAutorun.exe 开始 ISA Server 的安装。

（1）单击“安装 ISA Server 2004”，出现安装界面如图 4-33 所示。

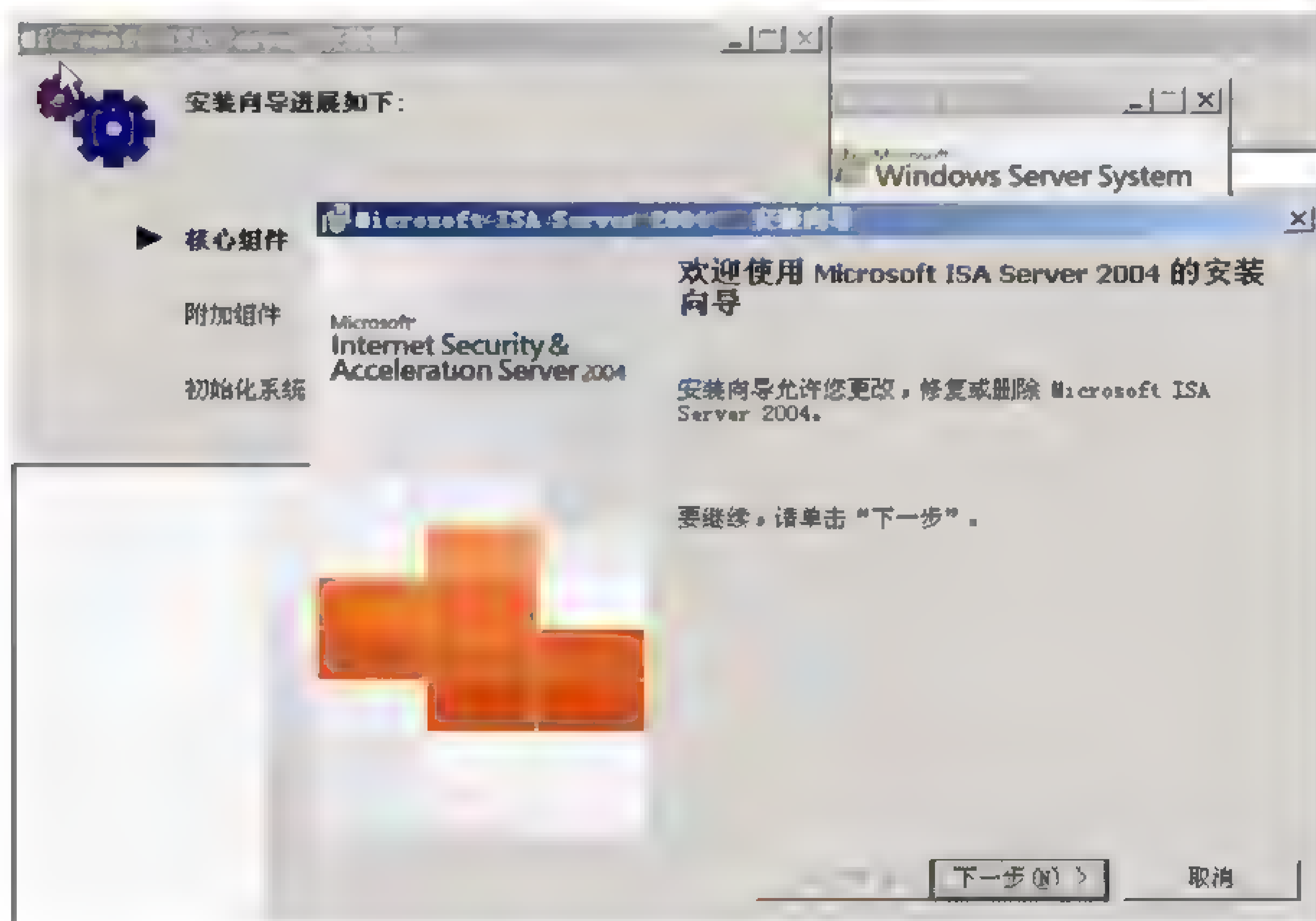


图 4-33　ISA 安装界面

（2）单击“下一步”按钮，在授权画面上选择“我接受许可协议中的条款”单选按钮，然后单击“下一步”按钮。在客户信息对话框，输入个人信息和产品序列号，单击“下一步”按钮继续。在图 4-34 安装类型对话框，如果你想改变 ISA Server 的默认安装选项，可以选择“自定义”单选按钮，然后单击“下一步”按钮。

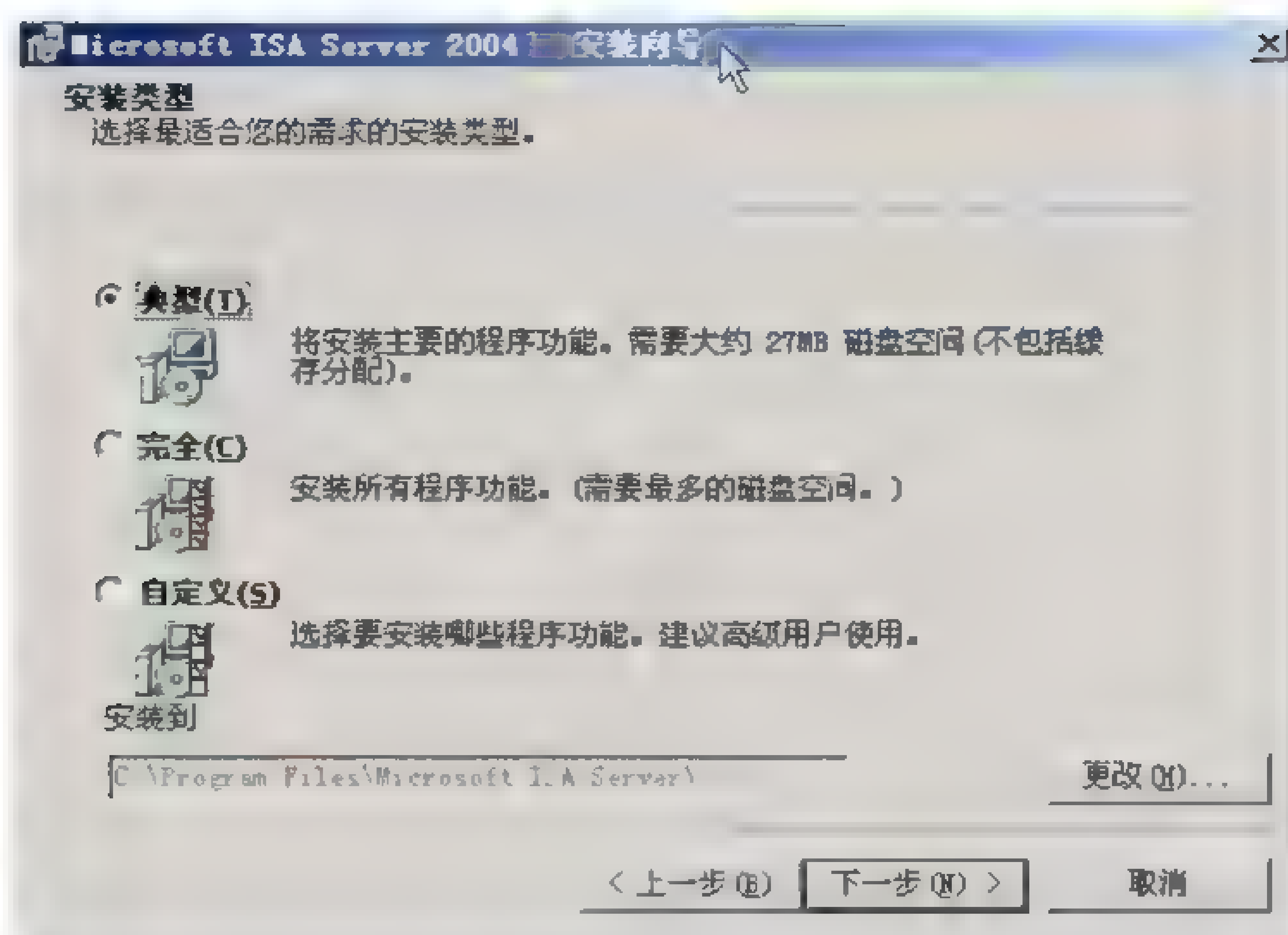


图 4-34　选择安装类型

（3）在图 4-35“自定义安装”对话框中可以选择安装的组件，默认情况下，会安装“防火墙服务器”和“ISA 服务器管理”，而“防火墙客户端安装共享”和用于控制垃圾邮件和邮件附件的“消息筛选程序”不会安装。如果想安装“消息筛选程序”，需要先在 ISA Server 2004 服务器上安装 IIS 6.0 SMTP 服务。单击“下一步”按钮继续。

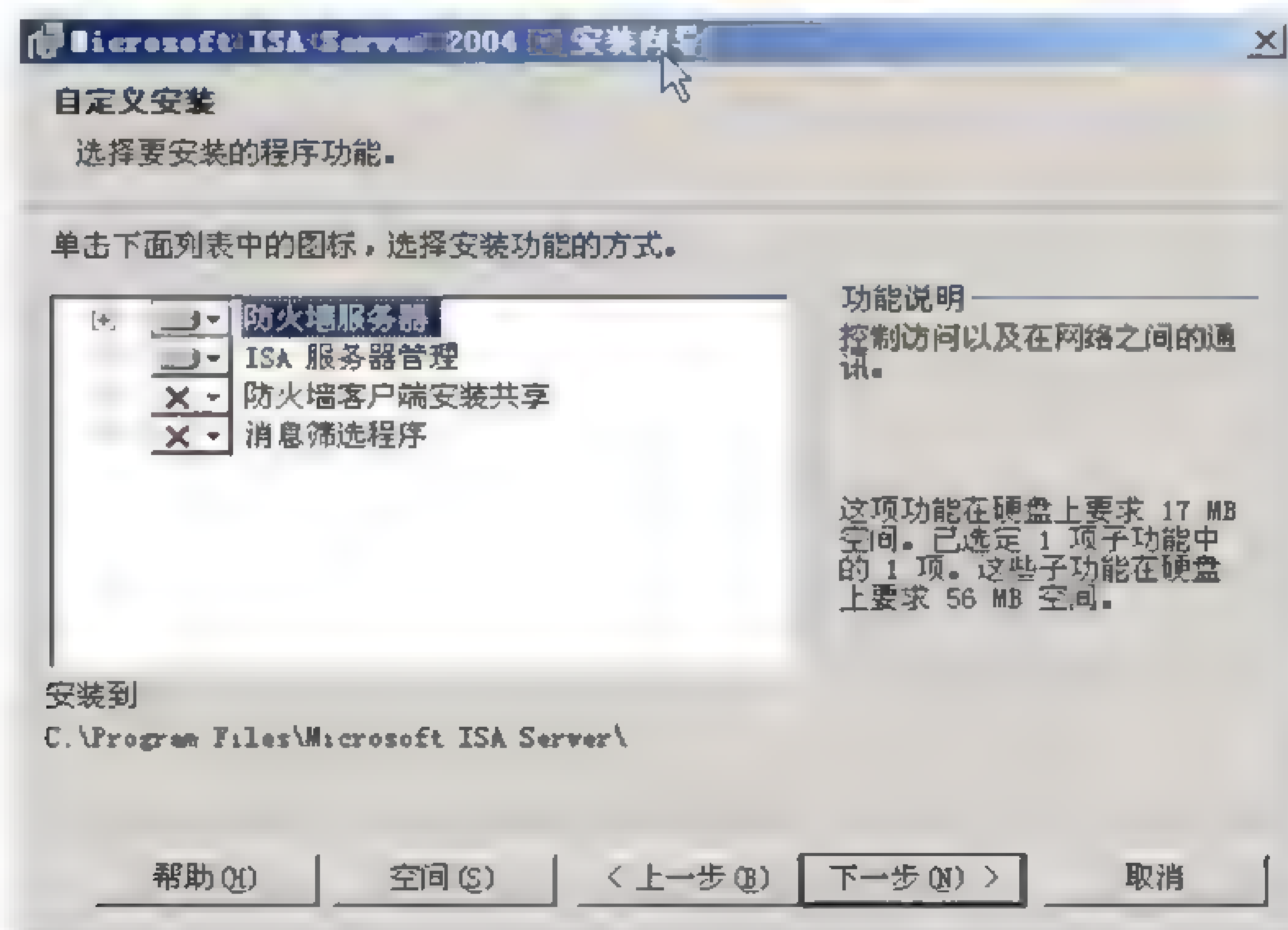


图 4-35　自定义安装

（4）在图 4-36“内部网络”对话框中，单击“添加”按钮。

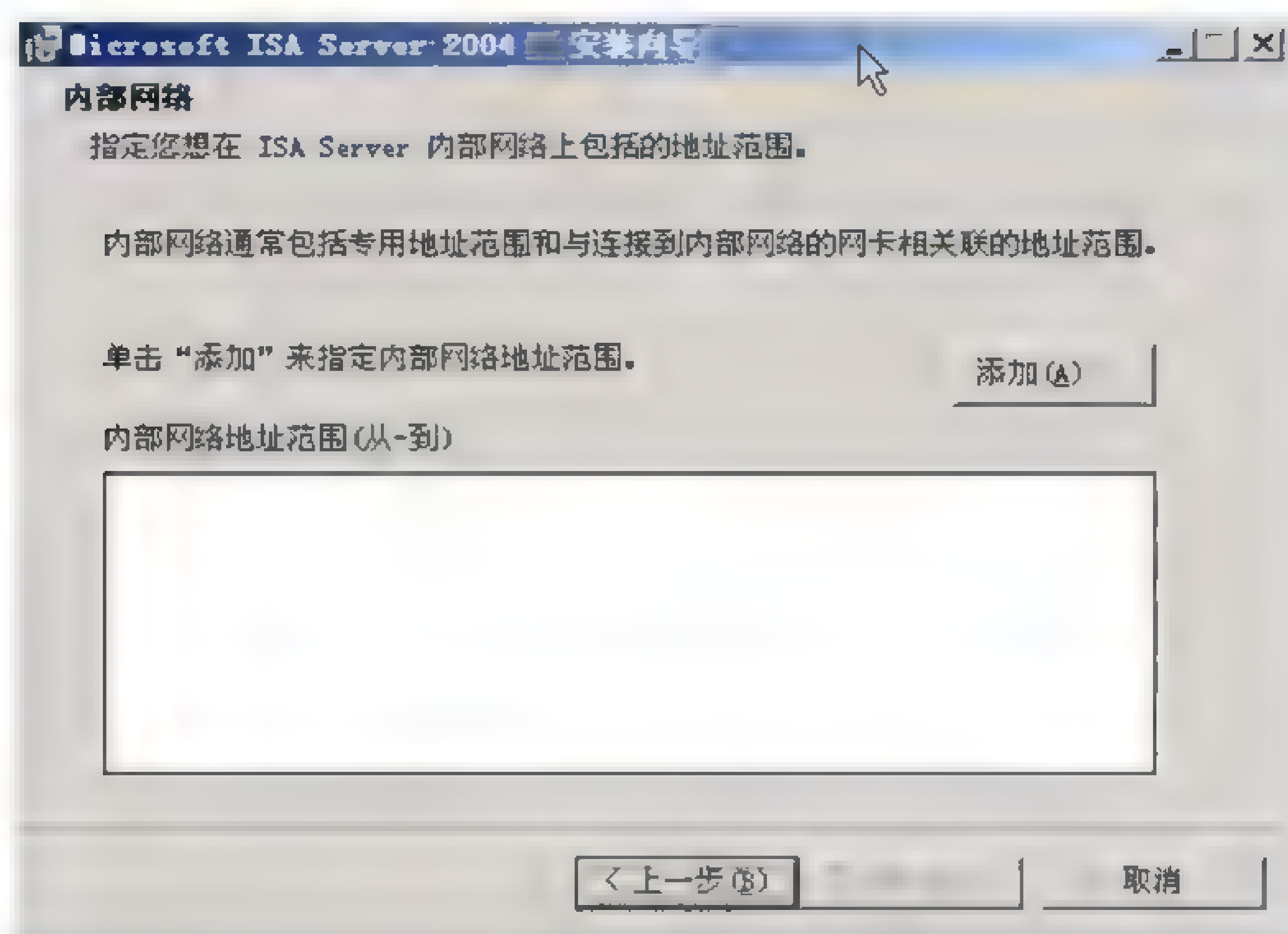


图 4-36　内部网络

内部网络和 ISA Server 2000 中使用的 LAT 已经大大不同了。在 ISA Server 2004 和 2006 中，内部网络定义为 ISA Server 必须进行数据通信的信任的网络。防火墙的系统策略会自动允许 ISA Server 到内部网络的部分通信。

（5）在图 4-37“地址添加”对话框中，单击“选择网卡”按钮，出现“选择网卡”对话框。

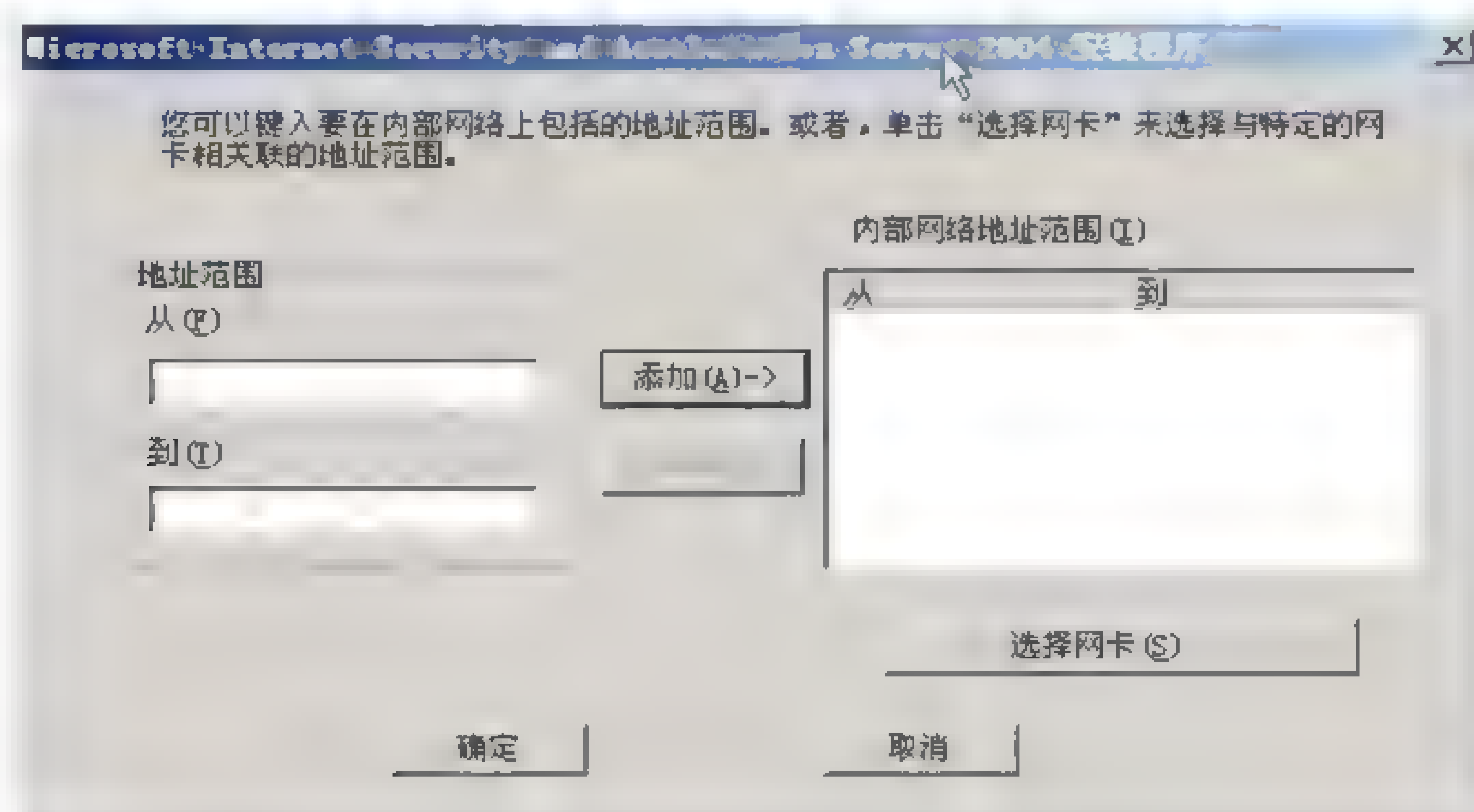


图 4-37　添加内部网络地址范围

（6）在图4-38“选择网卡”对话框中，取消对“添加下列专用范围：10.x.x.x，192.168.x.x，172.16.x.x-172.31.x.x 和 169.254.x.x。”复选框的勾选，保留对“基于 Windows 路由表添加地址范围”复选框的勾选，选择连接内部网络的适配器，单击“确定”按钮。在弹出的图 4-39 提示对话框中单击“确定”按钮。在内部网络地址对话框中单击“确定”按钮。

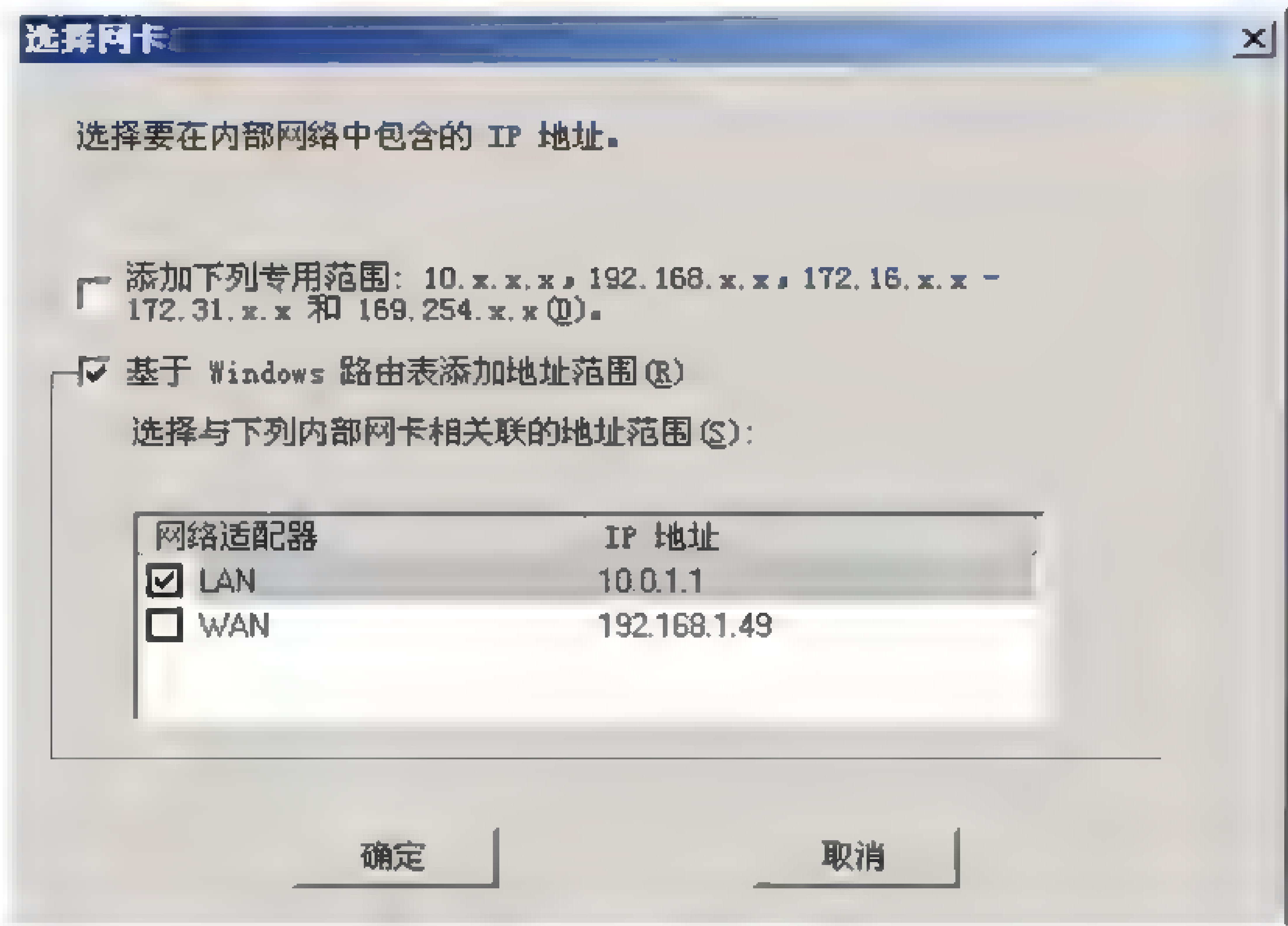


图 4-38　选择网卡

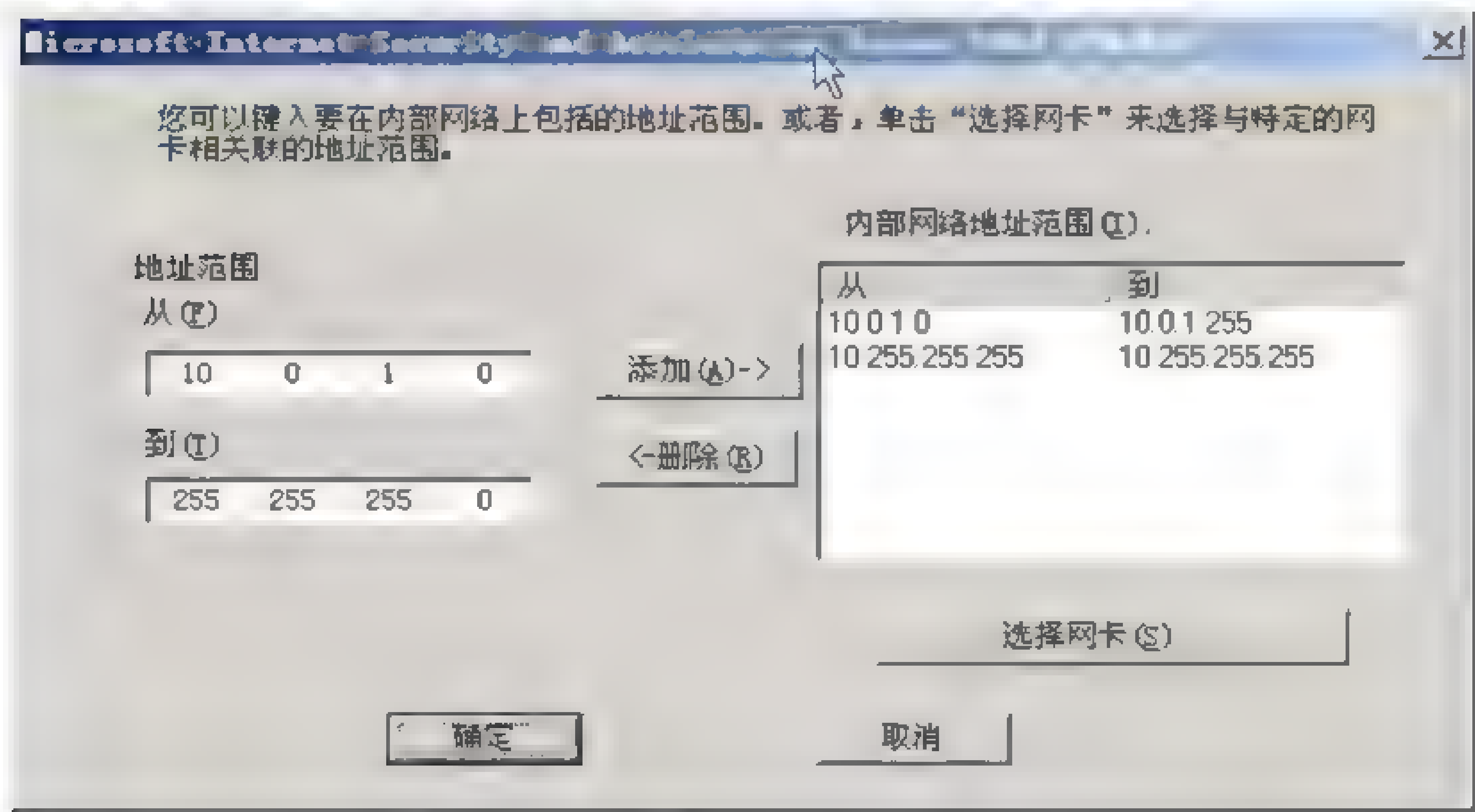


图 4-39　内部网络地址对话框

（7）然后在图 4-40“内部网络”对话框中单击“下一步”按钮。

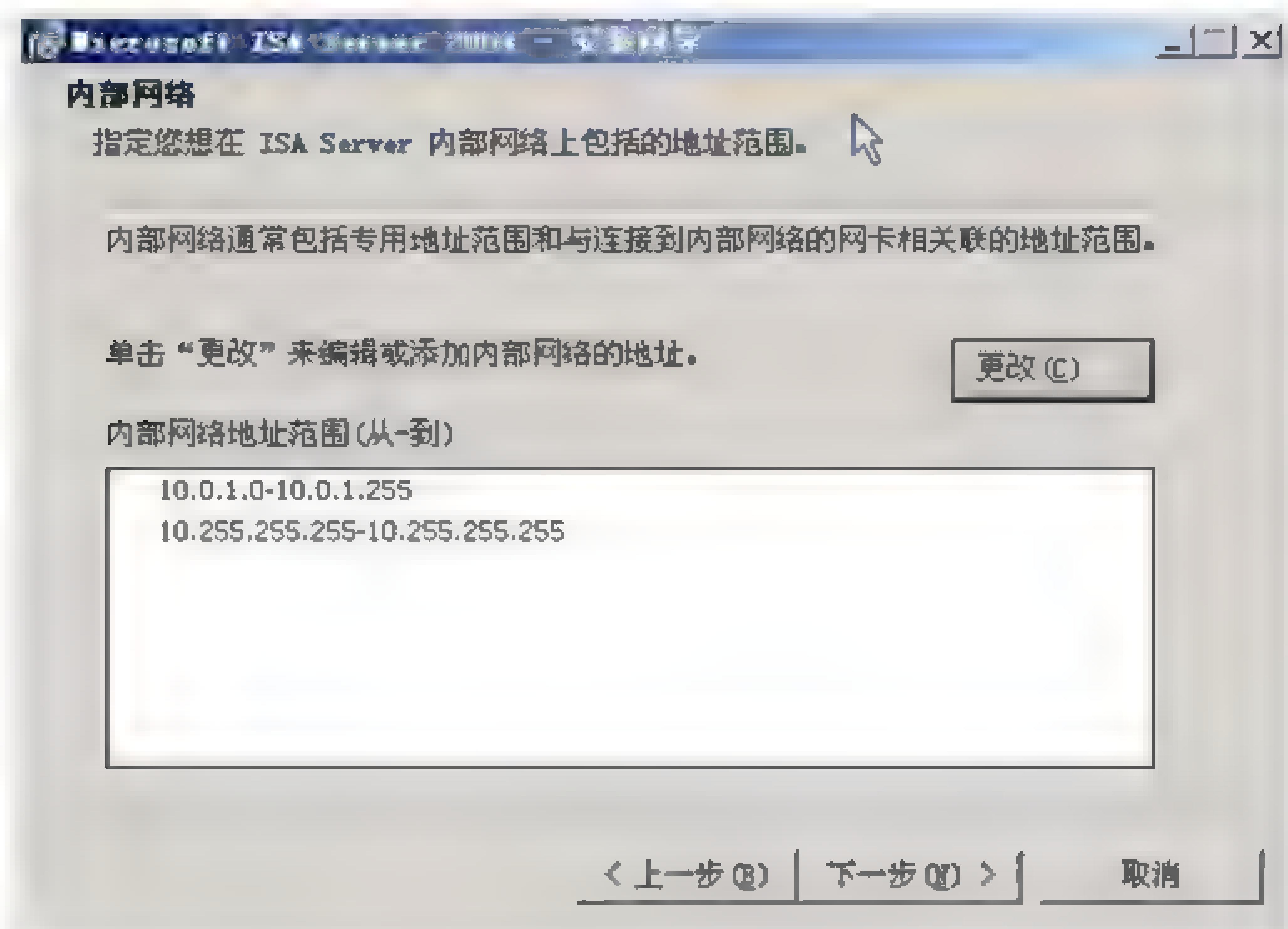


图 4-40　内部网络

（8）在图 4-41“防火墙客户端连接设置”对话框中，如果你的客户机上使用了 ISA Server 2000 的防火墙客户端，则可以选择“允许运行早期版本的防火墙客户端软件的计算机连接”复选框，然后单击“下一步”按钮。

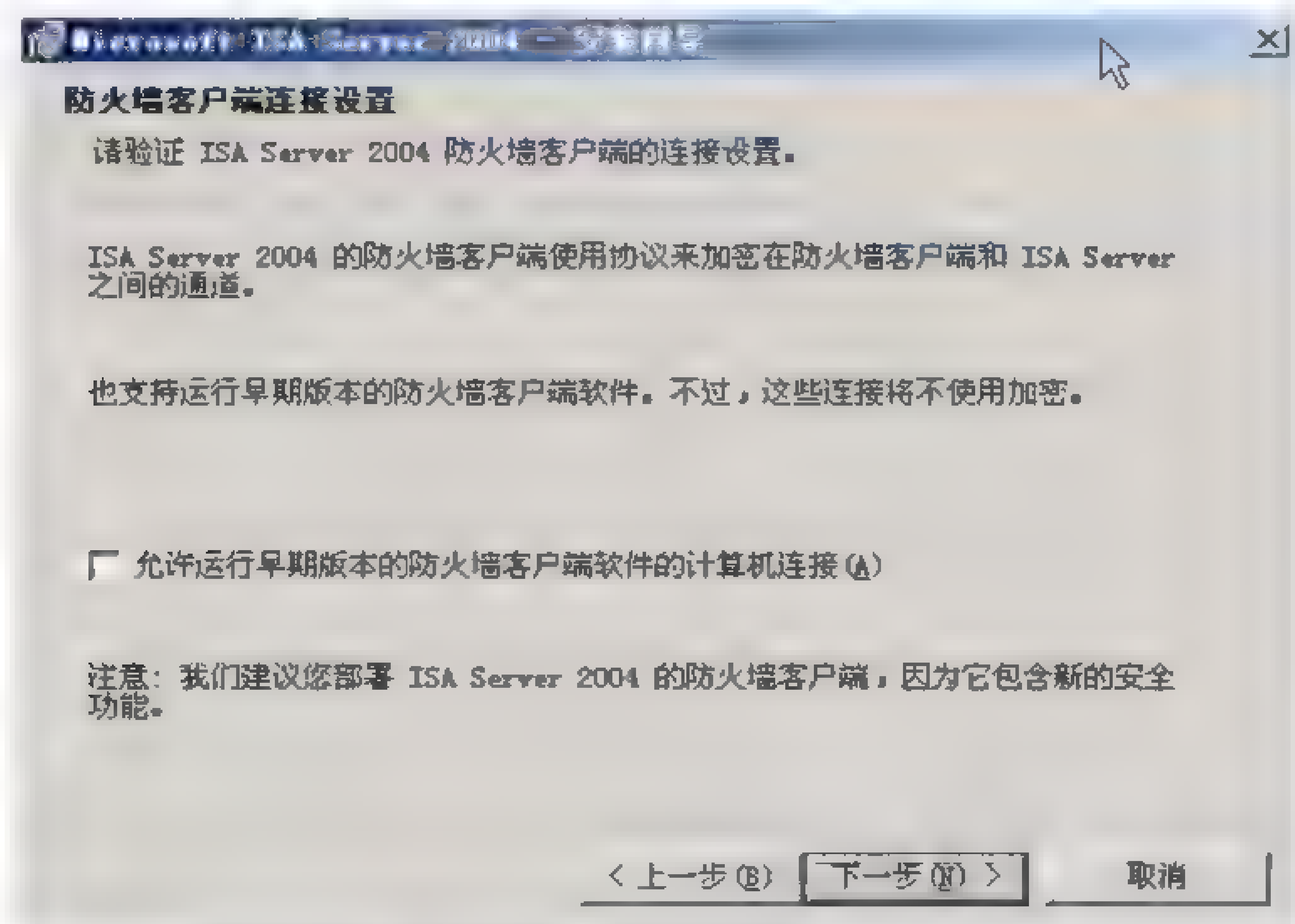


图 4-41　防火墙客户端连接设置

（9）在图 4-42“服务”对话框中单击“下一步”按钮。

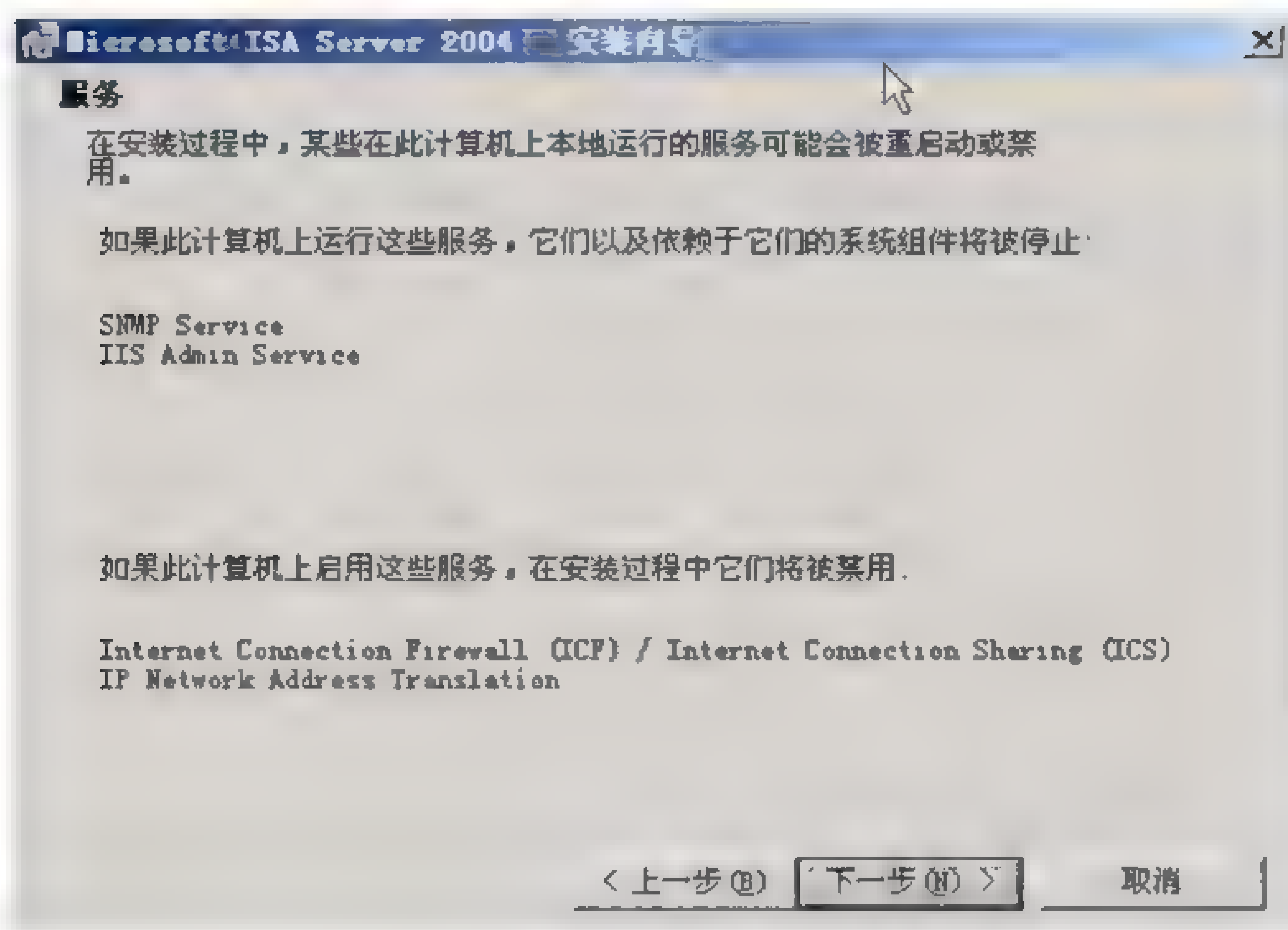


图 4-42　服务

（10）在“可以安装程序了”对话框中单击“安装”按钮。在“安装向导完成”对话框中，选择“在向导关闭时运行 ISA 服务器管理”单选按钮，然后单击“完成”按钮。此时，会出现 Microsoft Internet Security and Acceleration Server 2004 控制台。安装完毕。

4.4.2　配置允许所有内部用户访问 Internet 的所有服务的访问规则

1. 网络规则

在 ISA Server 中，防火墙策略是由网络规则、访问规则和服务器发布规则三者的结合组成的。网络规则定义了不同网络间是否能访问，以及如果可以访问则该如何进行访问；访问规则定义了用户（内、外网）的访问；服务器发布规则定义了如何让用户访问服务器。

网络规则是 ISA Server 中的一个重大改进，通过网络规则来定义并描述网络拓扑，可以很好地支持复杂的网络环境。网络规则确定两个网络之间是否存在连接，以及定义如何进行连接。网络连接的方式如下。

（1）路由。当指定这种类型的连接时，来自源网络的客户端请求将被直接转发到目标网络。源客户端地址包含在请求中。当发布位于 DMZ 网络中的服务器时，可以使用路由网络规则。

（2）网络地址转换（NAT）。当指定这种类型的连接时，ISA 服务器将用它自己的 IP 地址替换源网络中客户端的 IP 地址。当定义内部网络与外部网络之间的关系时，可

以使用 NAT 网络规则。

路由网络关系是双向的。如果定义了从网络 A 到网络 B 的路由关系，那么从网络 B 到网络 A 也存在着路由关系。相反，NAT 关系则是唯一的和单向的。如果定义了从网络 A 到网络 B 的 NAT 关系，则不能定义从网络 B 到网络 A 的网络关系。用户可以创建定义双向关系的网络规则，但是 ISA 服务器将忽略有序规则列表中的第二条网络规则。

安装时，会创建图 4-43 所示默认规则。

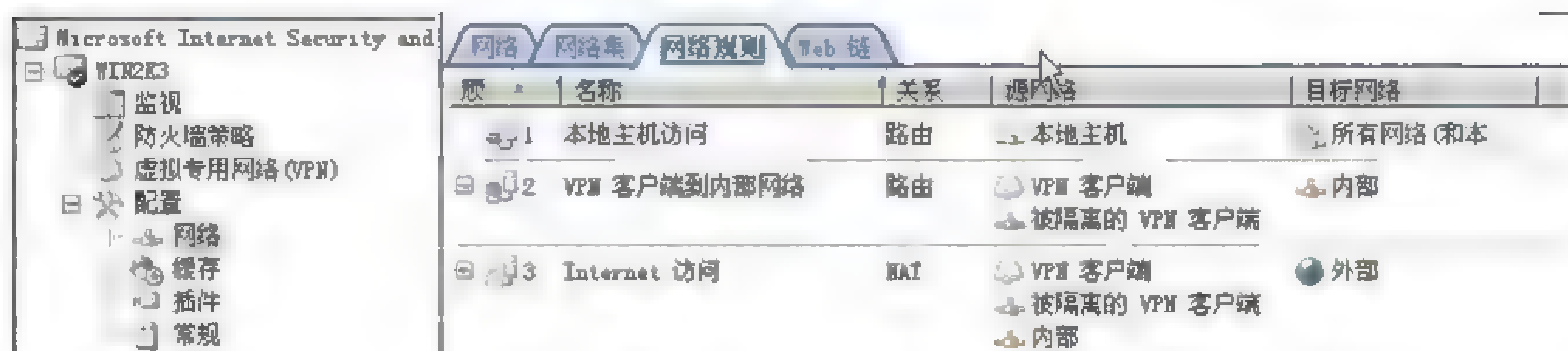


图 4-43　网络规则

（3）本地主机访问。此规则定义了在本地主机网络与其他所有网络之间存在的路由关系。

（4）VPN 客户端到内部网络。此规则指定在两个 VPN 客户端网络（“VPN 客户端”和“被隔离的 VPN 客户端”）与内部网络之间存在着路由关系。

（5）Internet 访问。此规则定义了在内部受保护的网络（如内部、VPN 客户端等）与外部网络之间存在的 NAT 关系。

2．访问规则

1）防火墙系统策略

在安装 ISA Server 服务器时，会创建默认的系统策略。系统策略允许 ISA Server 服务器访问它连接到的网络的特定服务。在图 4-44 所示“防火墙策略”上单击右键，从弹出的快捷菜单中选择“查看”→“显示系统策略规则”命令，可以查看系统策略。如图 4-45 所示。

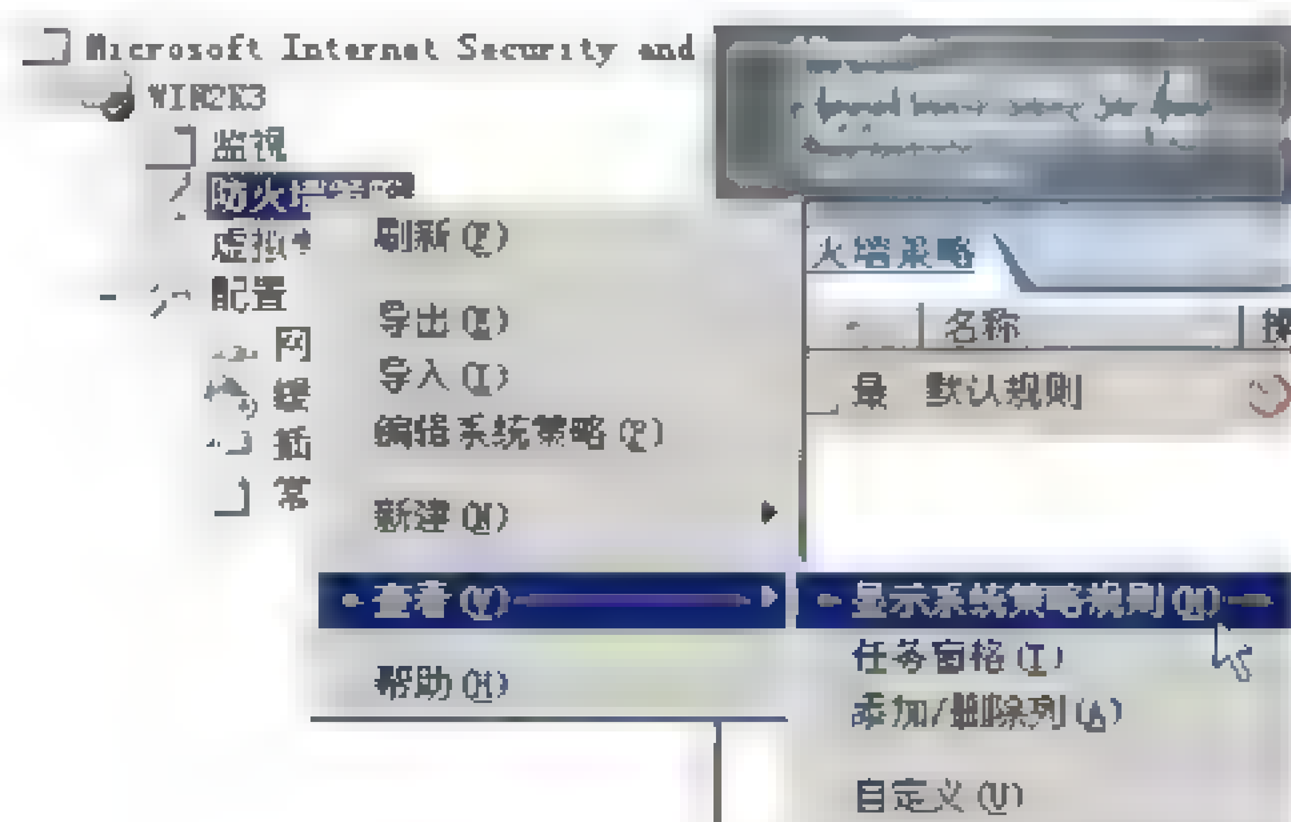


图 4-44　查看系统策略

标注的地方表明 ISA Server 服务器可以向任何网络发起 DNS 请求。



图 4-45　防火墙策略

2）建立访问策略

从 ISA Server 2004 开始不要求必须为用户所访问的服务定义协议，只需要一条策略就可以让内部客户完全地访问 Internet 上的所有服务。

为了方便使用，ISA Server 2004 附带了网络模板的功能，使用也很简单。还可以通过 ISA Server 的规则向导，轻松地建立访问策略。

根据目前的网络环境，需要两条策略：一条访问策略，以允许内部网络客户访问外部网络（Internet）；同时，因为内部网络客户需要访问 ISA Server 服务器上的 DNS 服务器以解析域名，也需要建立一条策略以允许内部网络客户访问 ISA Server 服务器的 DNS 服务。首先，新建一条允许内部客户访问外部网络的所有服务的访问规则。

（1）在“防火墙策略”上单击右键，从弹出的快捷菜单中选择“新建”→“访问规则”命令。如图 4-46 所示。

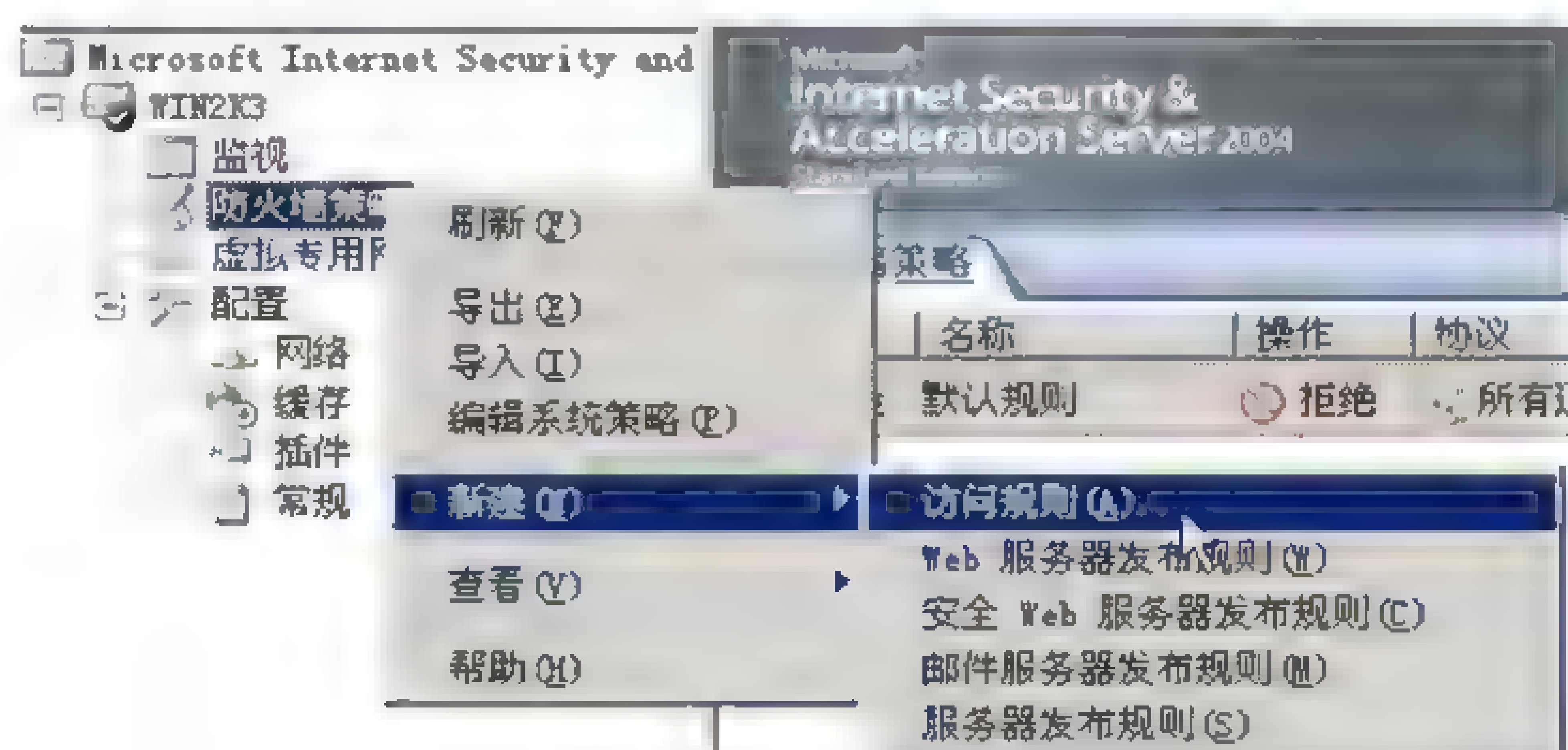


图 4-46　建立访问策略

（2）在图 4-47“新建访问规则向导”对话框的访问规则名称文本框中输入 Allow all outbound traffic，然后单击“下一步”按钮。然后在“规则操作”对话框中选择“允许”单选按钮，单击“下一步”按钮。

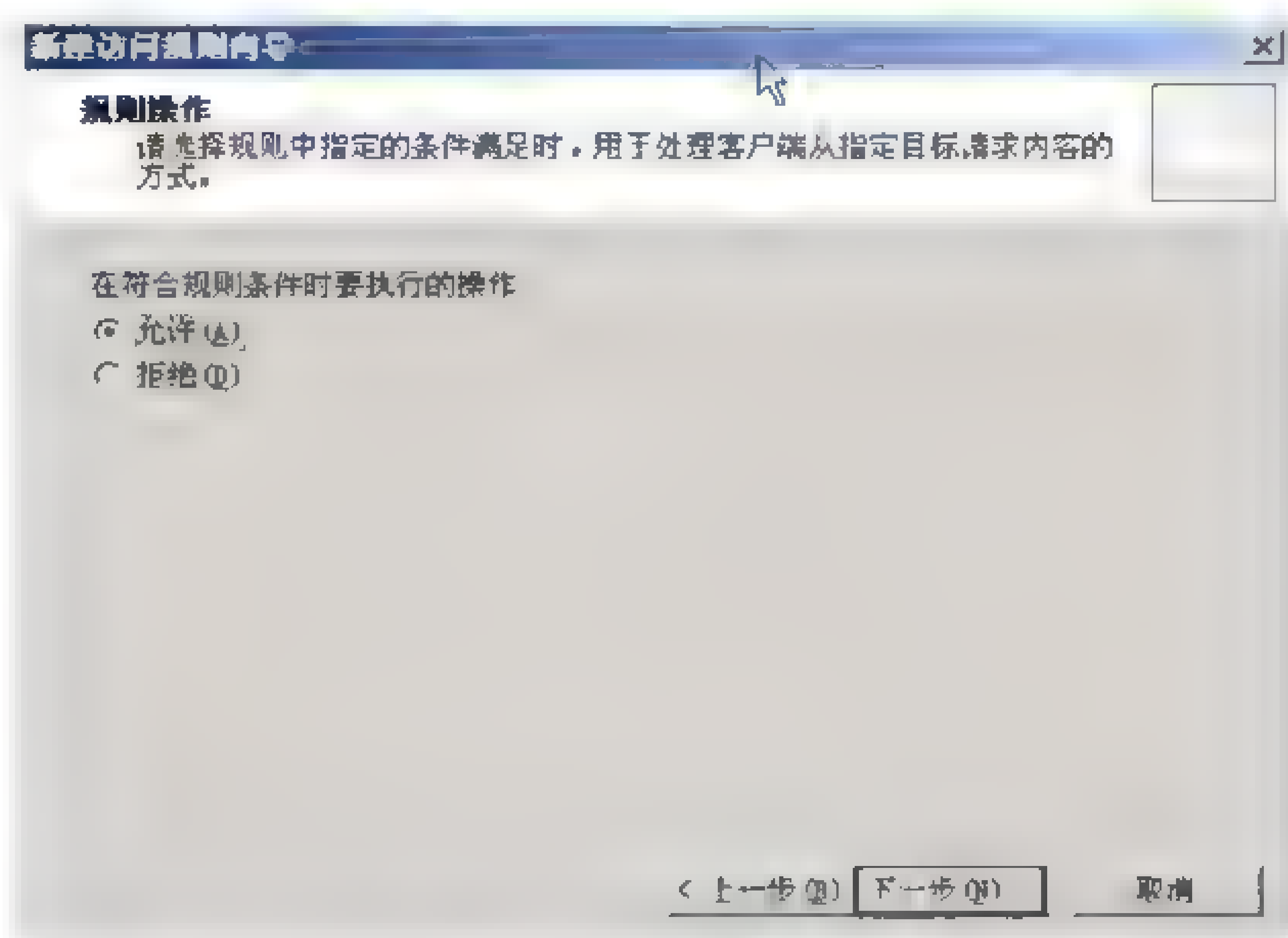


图 4-47　新建访问规则

（3）在图 4-48“协议”对话框中的“此规则应用到”下拉列表框中选择“所有出站讯”选项，单击“下一步”按钮。

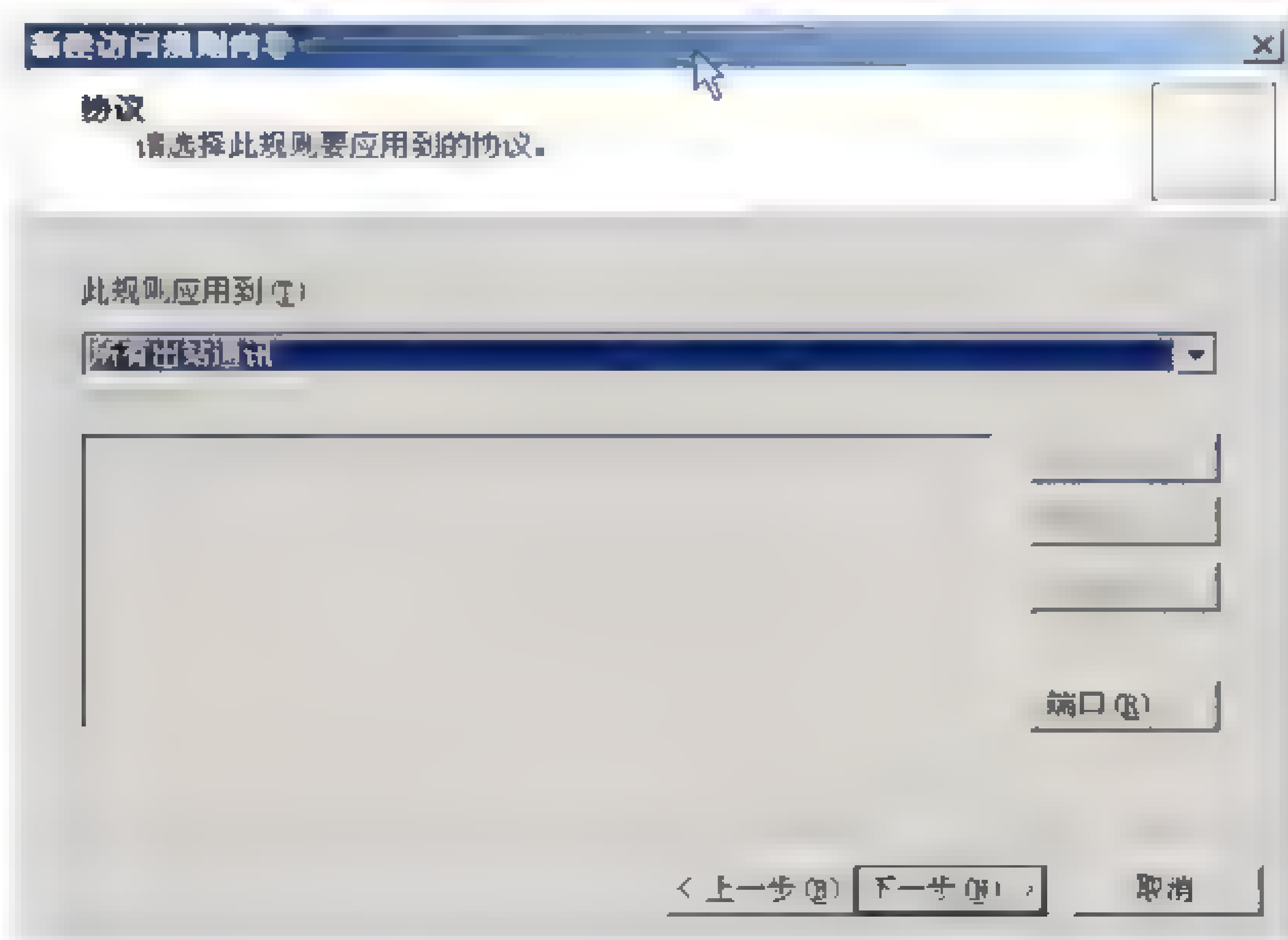


图 4-48　选择应用的协议

（4）在图 4-49“访问规则源”对话框中单击“添加”按钮，在打开的“添加网络实体”对话框中双击“内部”项，然后单击“关闭”按钮，回到“访问规则源”对话框单击“下一步”按钮。

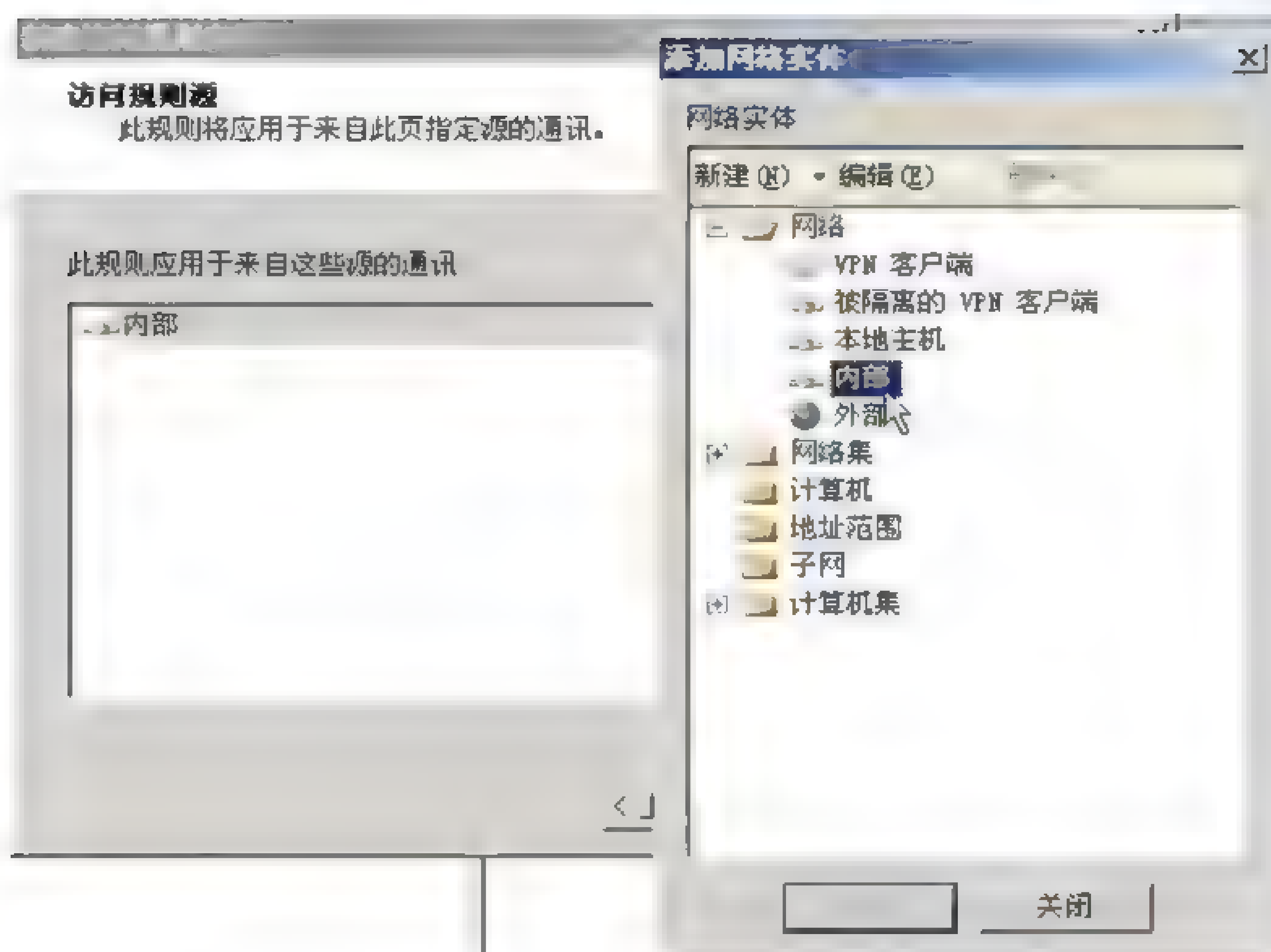


图 4-49 访问规则源

（5）在图 4-50“访问规则目标”对话框中单击“添加”按钮，在“添加网络实体”对话框中双击“外部”项，然后单击“关闭”按钮，回到“访问规则目标”对话框中单击“下一步”按钮。

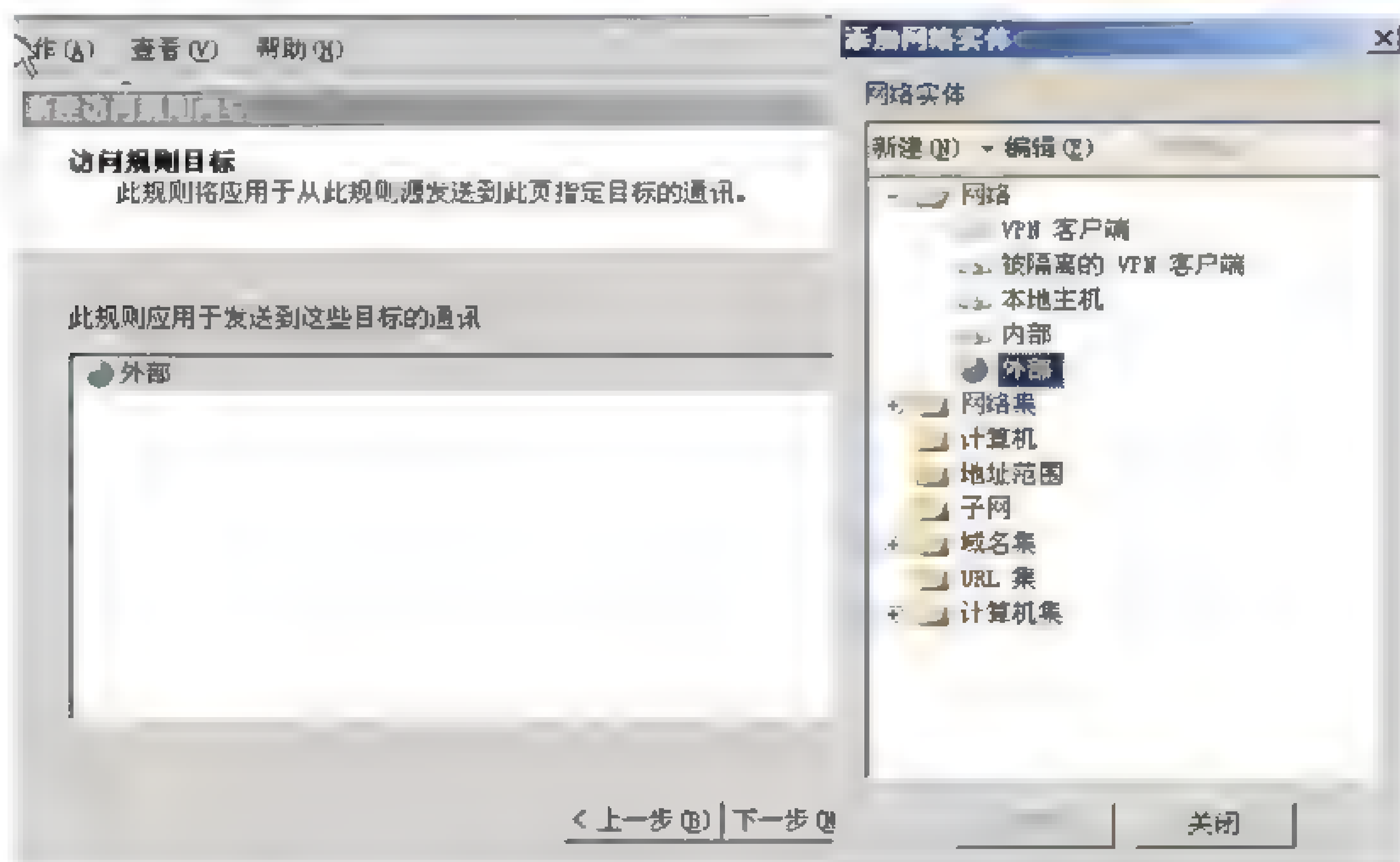


图 4-50 访问规则目标

（6）在图 4-51“用户集”对话框中接受默认的所有用户，然后单击“下一步”按钮。

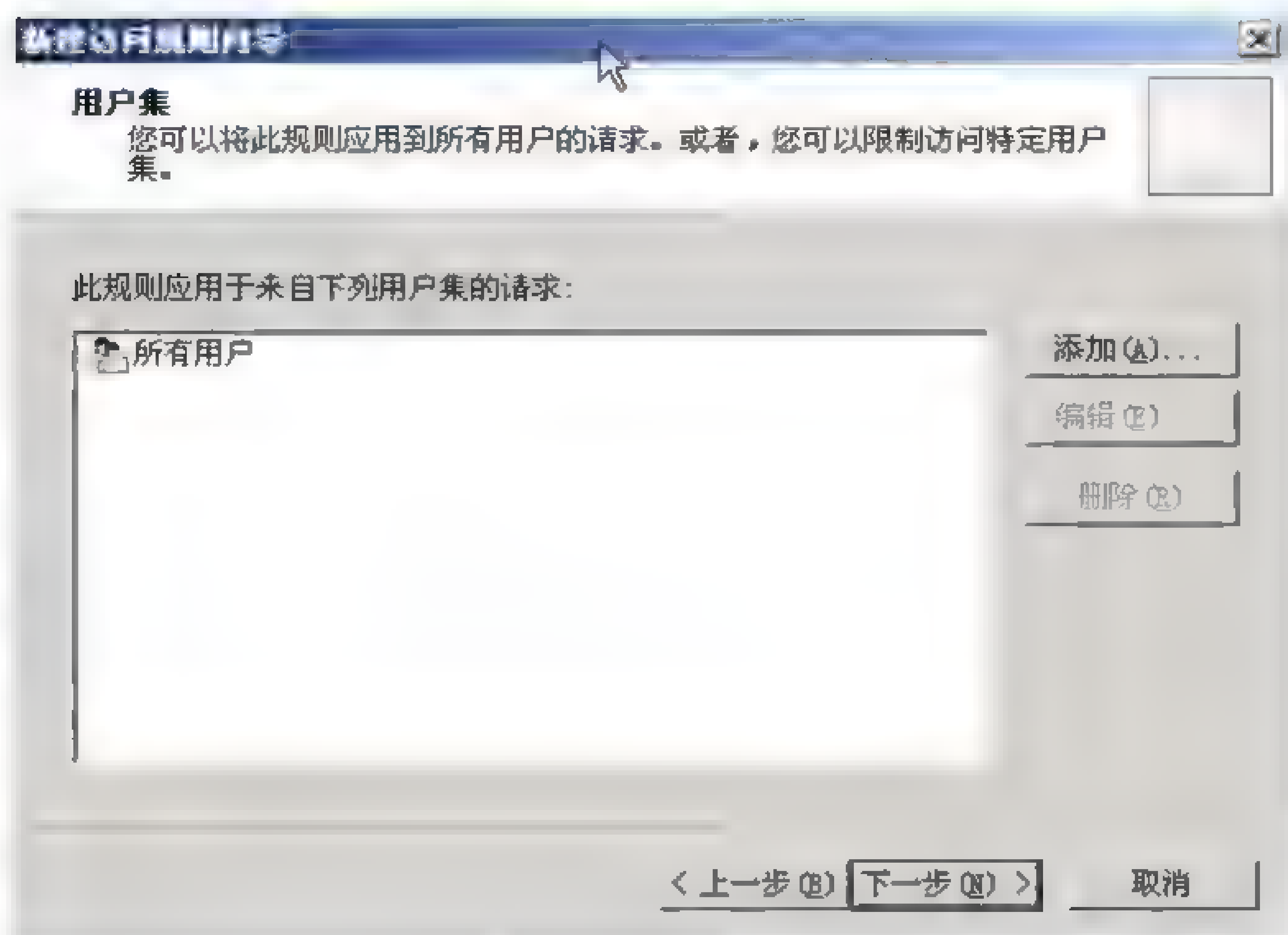


图 4-51　用户集

（7）在“完成新建访问规则向导”对话框中单击“完成”按钮。

然后，新建一条允许内部客户访问 ISA Server 2004 服务器上的 DNS 服务的访问规则。这条规则的步骤和上面一条一样，不同的地方在“规则名：Allow internal access firewall's dns service”。

（1）在图 4-52“协议”对话框中的“此规则应用到”下拉列表框中选择“所选的协议”选项，然后单击“添加”按钮，在打开的“添加协议”对话框中选择“通用协议”节点下的 DNS。

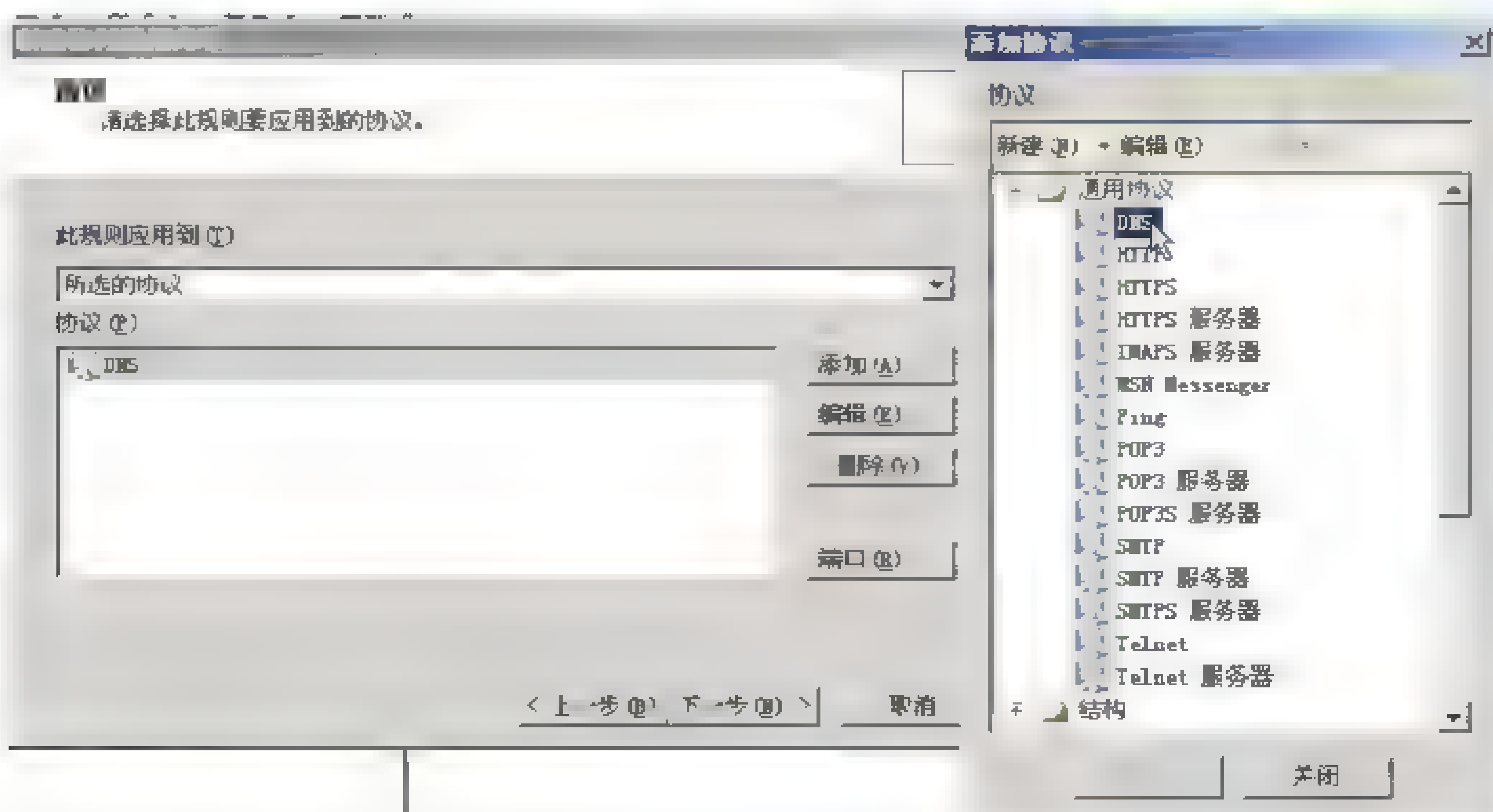


图 4-52　选择应用到的协议

（2）在图 4-53“访问规则目标”对话框中单击“添加”按钮，在打开的“添加网络实体”对话框中选择“本地主机”，单击“添加”按钮，然后在“访问规则目标”对话框中单击“下一步”按钮。

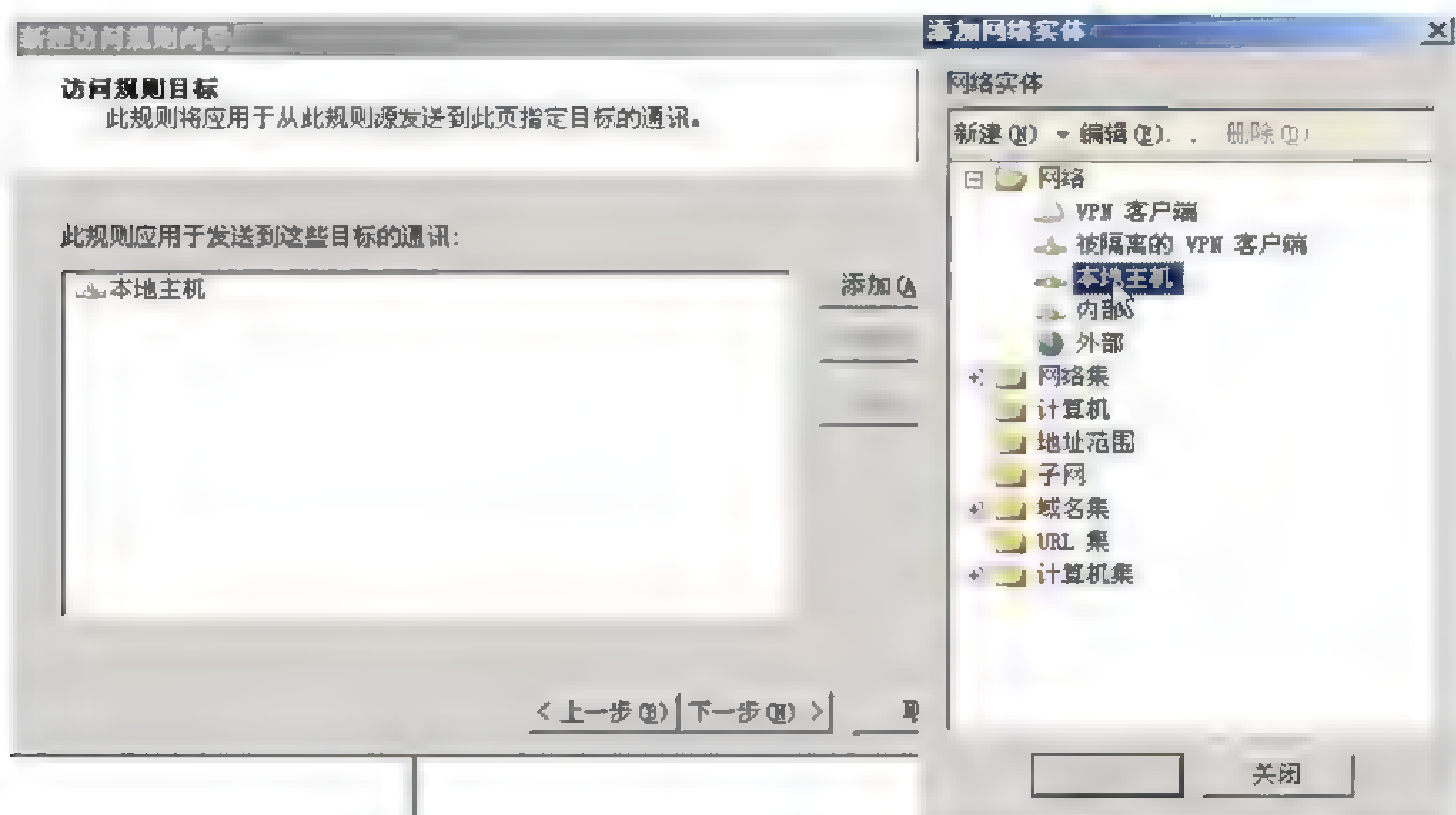


图 4-53 访问规则目标

（3）此时，ISA Server 2004 的管理控制台应该如图 4-54 所示，单击“应用”按钮以保存修改和更新防火墙策略。

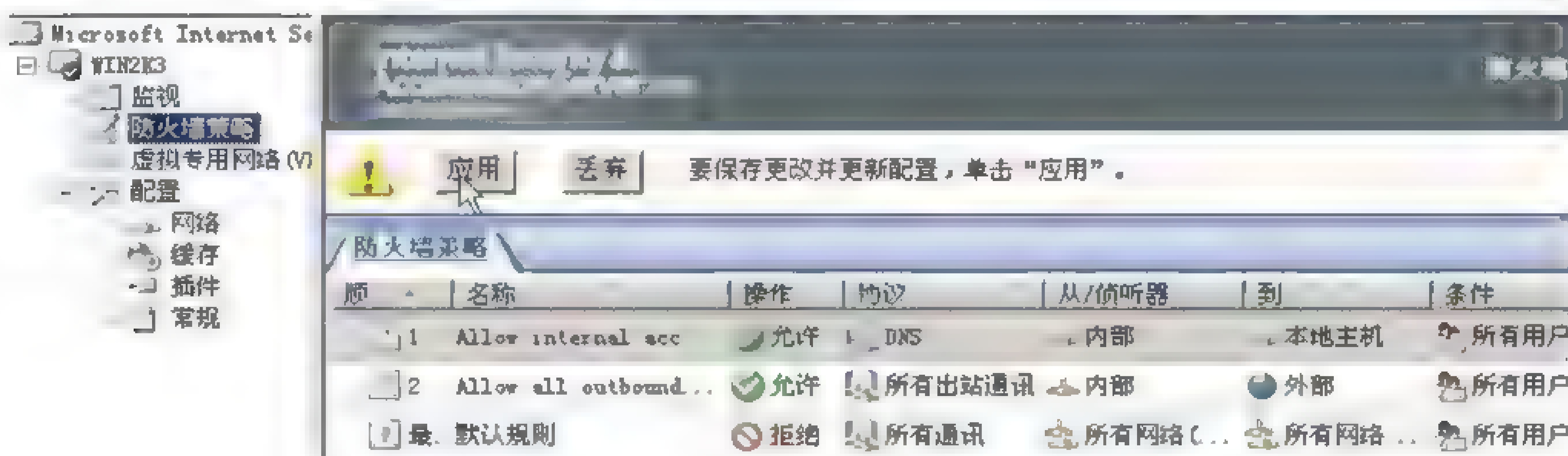


图 4-54 应用新防火墙策略

（4）在图 4-55“应用新配置”对话框中单击“确定”按钮。

此时，ISA Server 服务器的初步配置已经完成，内部客户可以访问外部网络的所有服务，也可以访问 ISA Server 2004 服务器上的 DNS 服务。注意：只能访问 ISA Server 2004 服务器上的 DNS 服务，其他的服务都会被禁止（如 ping 等），因为还没有在策略中明确

允许这一点。

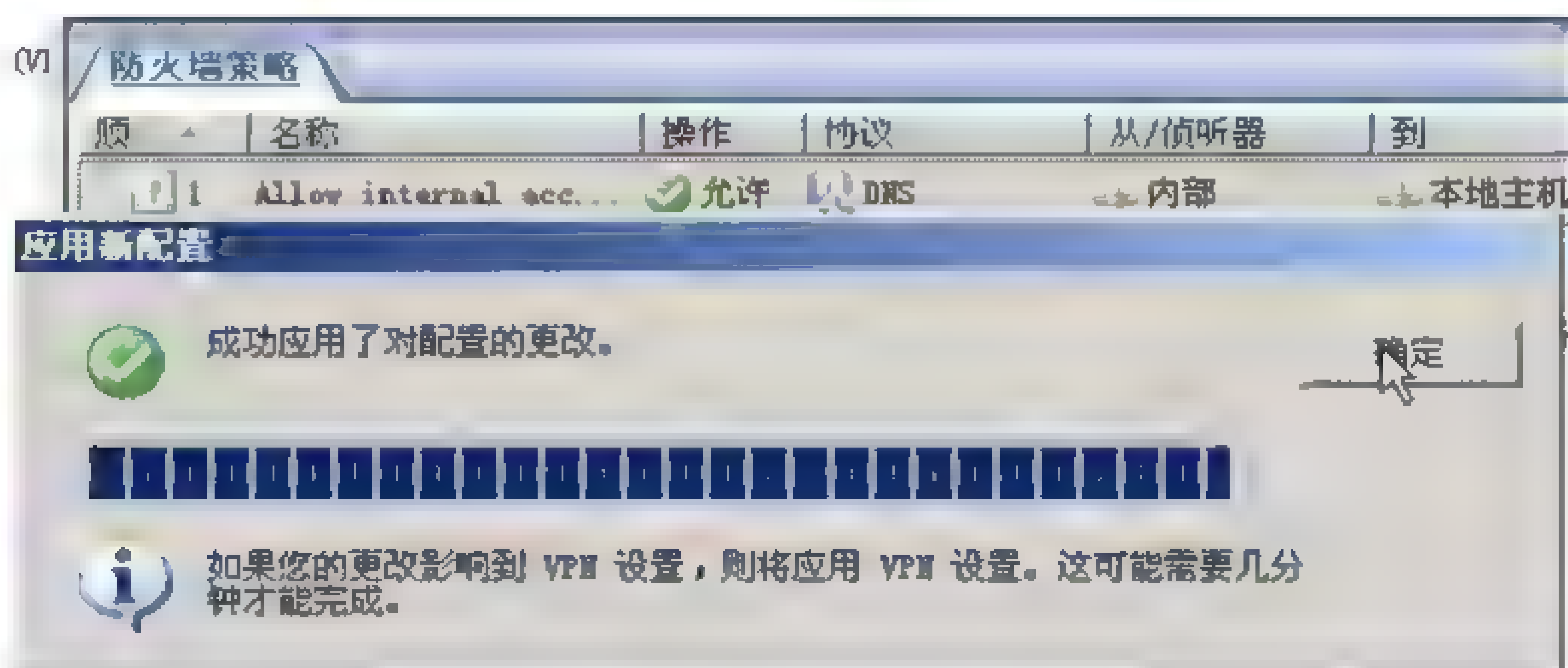


图 4-55　应用新配置

如果网络具有 Internet 的静态 IP，那么，在这一步网络已经可以正常工作了；如果是需要拨号登录 Internet 的网络，还需要设置请求拨号。

3．配置拨号连接

在 ISA Server 中，配置请求拨号非常简单。

（1）把拨号对象建立好，这个是在 Windows 的网络连接里面进行的。拨号对象建立好后，进入 ISA Server 管理控制台，展开服务器对象，单击“常规”，然后单击右边的“指定拨号首选项”链接，如图 4-56 所示。



图 4-56　ISA 服务器管理

（2）在图 4-57“拨号配置”对话框中，首先选择“允许自动拨此网络”单选按钮，允许 ISA Server 进行请求拨号，然后在下拉列表框里面选择“外部”选项。然后勾选“将此拨号连接配置为默认网关”复选框，在“拨号连接”选项区域中单击“选择”按钮，选择拨号项，这里选择已经建立好的宽带拨号项“China telecom”。

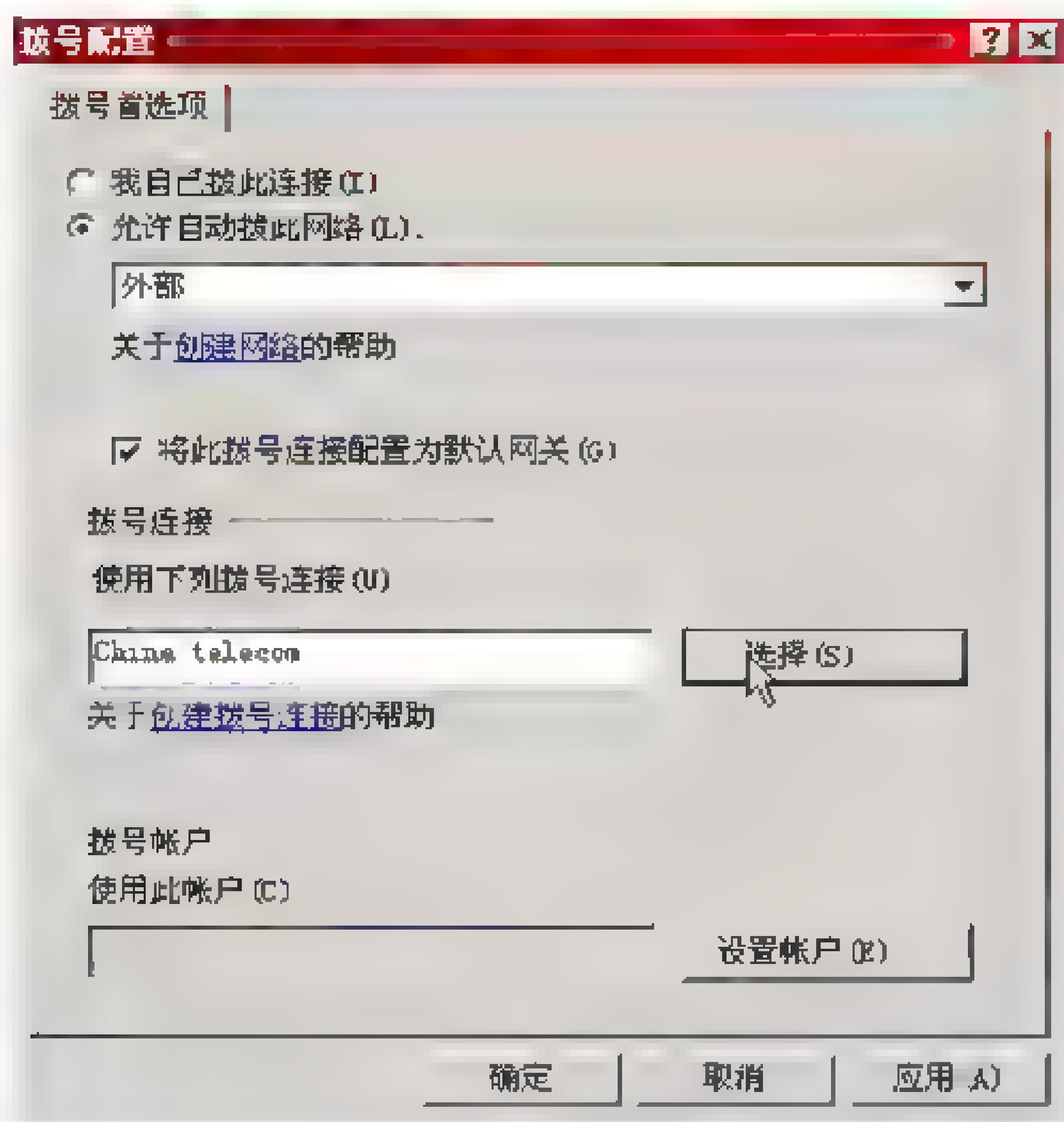


图 4-57　拨号配置

（3）单击“设置账户”按钮，弹出对话框如图 4-58 所示。

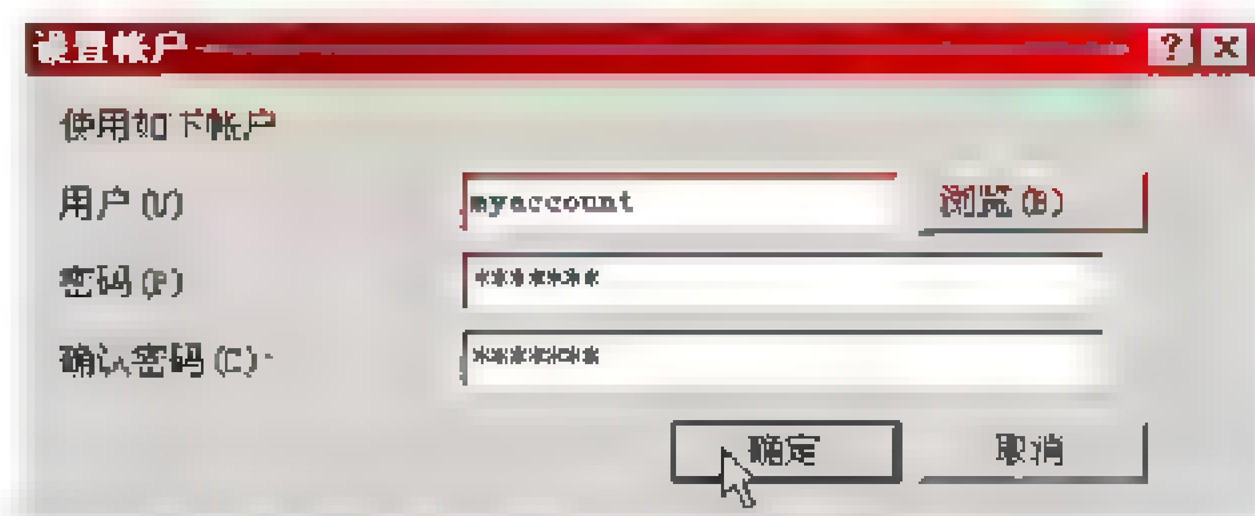


图 4-58　设置账户

（4）输入用户名和密码后，单击“确定”按钮，最后在 ISA 管理控制台单击“应用”按钮以保存修改和更新防火墙策略。这时，ISA Server 的请求拨号就配置好了。

4.4.3　使用边缘防火墙模板建立访问策略

除了常见的各种配置向导外，ISA Server 还提供了网络模板，可以设置防火墙策略。下面以适用范围最广的边缘防火墙策略为例来建立防火墙策略，如图 4-59 所示。

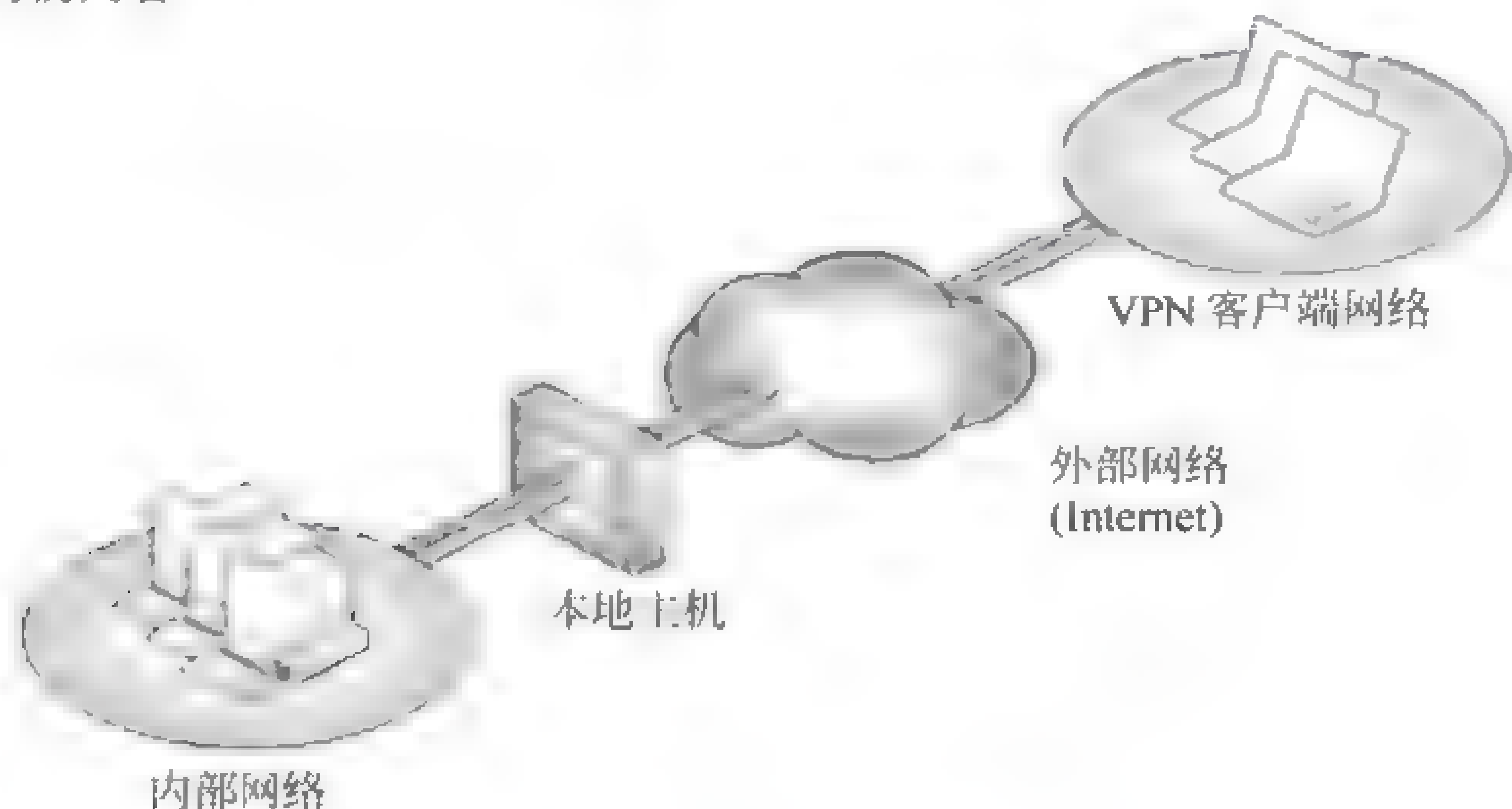


图 4-59　边缘防火墙应用

（1）打开 ISA Server 管理控制台，展开服务器，再展开“配置”，单击“网络”，如果任务面板没有打开，单击“打开/关闭任务栏”按钮打开任务面板。在任务面板，选择“模板”标签，单击“边缘防火墙”模板。如图 4-60 所示。



图 4-60　应用边缘防火墙模板

（2）在“欢迎使用网络模板向导”对话框中单击“下一步”按钮。在图 4-61“导出 ISA 服务器的配置”对话框中，如果过去没有保存过配置，可以单击“导出”按钮保存当前配置。在此直接单击“下一步”按钮。

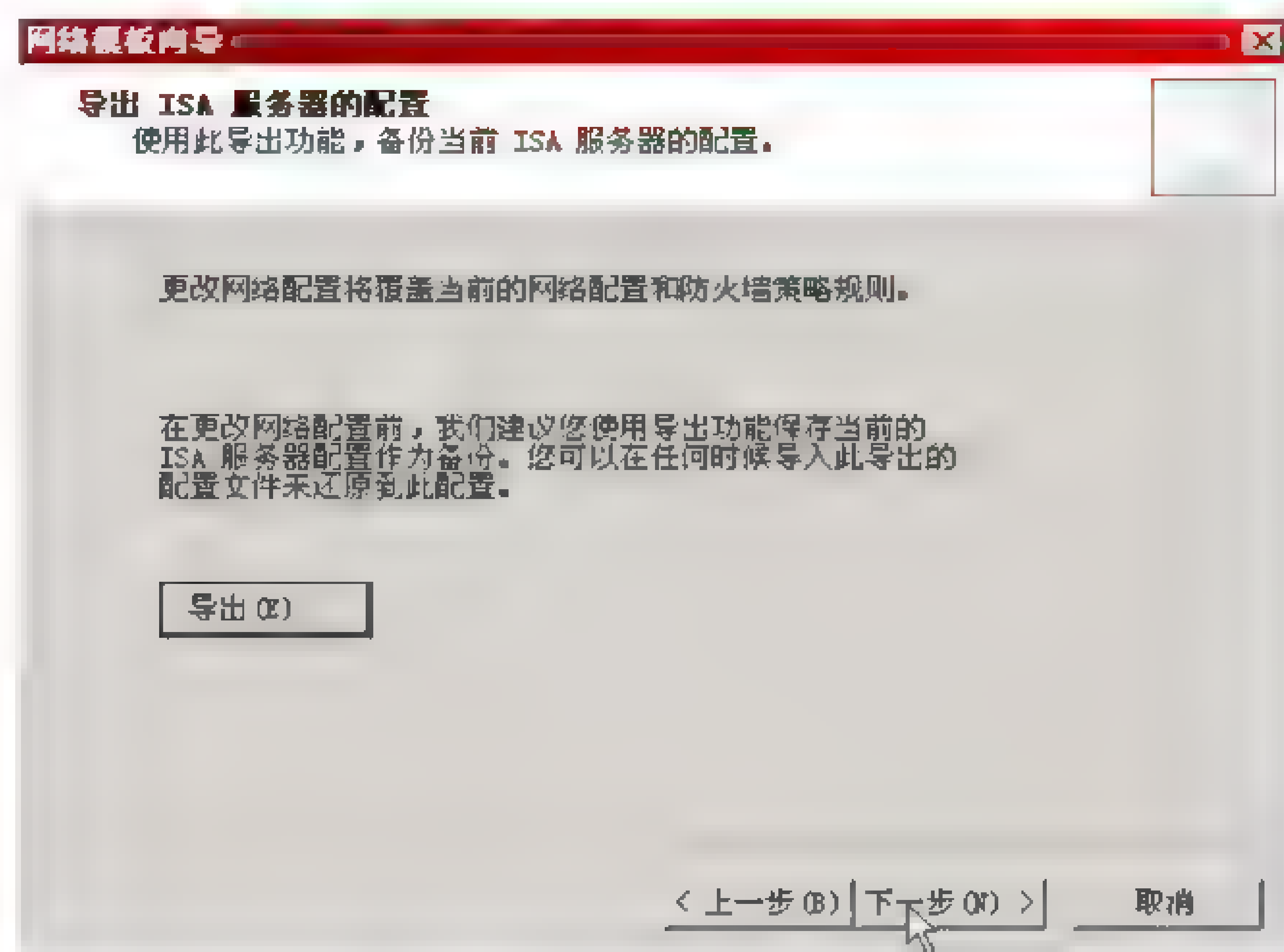


图 4-61　导出 ISA 服务器的配置

（3）在图 4-62“内部网络 IP 地址”对话框中，确认向导正确识别了内部网络的 IP 地址。可以使用添加、添加适配器或者添加专用按钮来添加更多的 IP 地址。在“地址范围”列表框内的 IP 地址将在后面向导配置的防火墙中允许访问外部网络。在所有的 IP 地址都添加完毕后，单击“下一步”按钮继续。

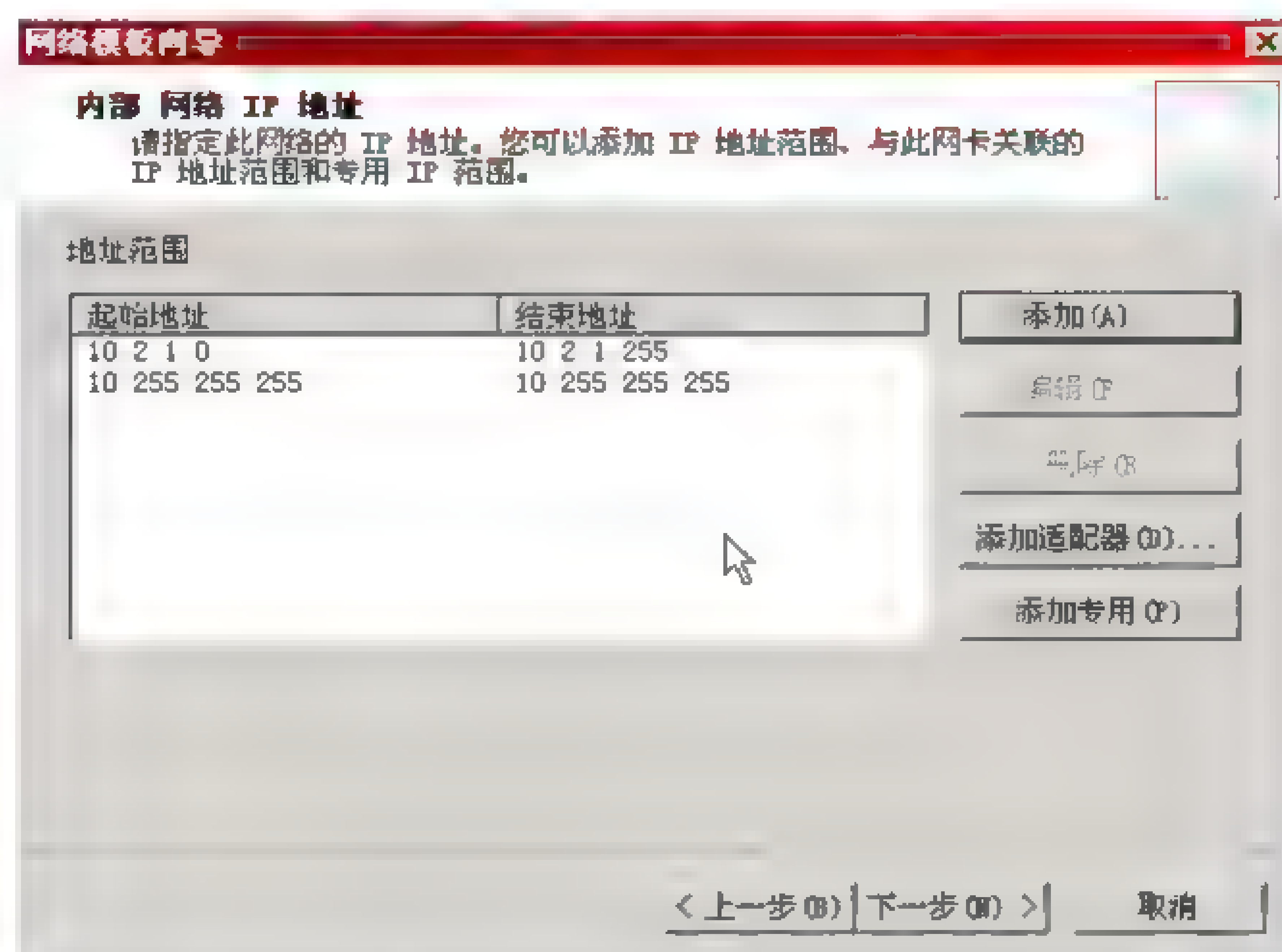


图 4-62　内部网络 IP 地址

（4）在图 4-63“选择一个防火墙策略”对话框中，从“选择一个防火墙策略”列表框中选择一个防火墙策略。在这个例子中，选择“允许无限制的访问”，这个防火墙策略将允许内部网络和 VPN 客户网络的主机完全访问 Internet（建立的策略除了包含有 VPN 客户外，基本和刚才建立的策略一样），然后单击“下一步”按钮继续。

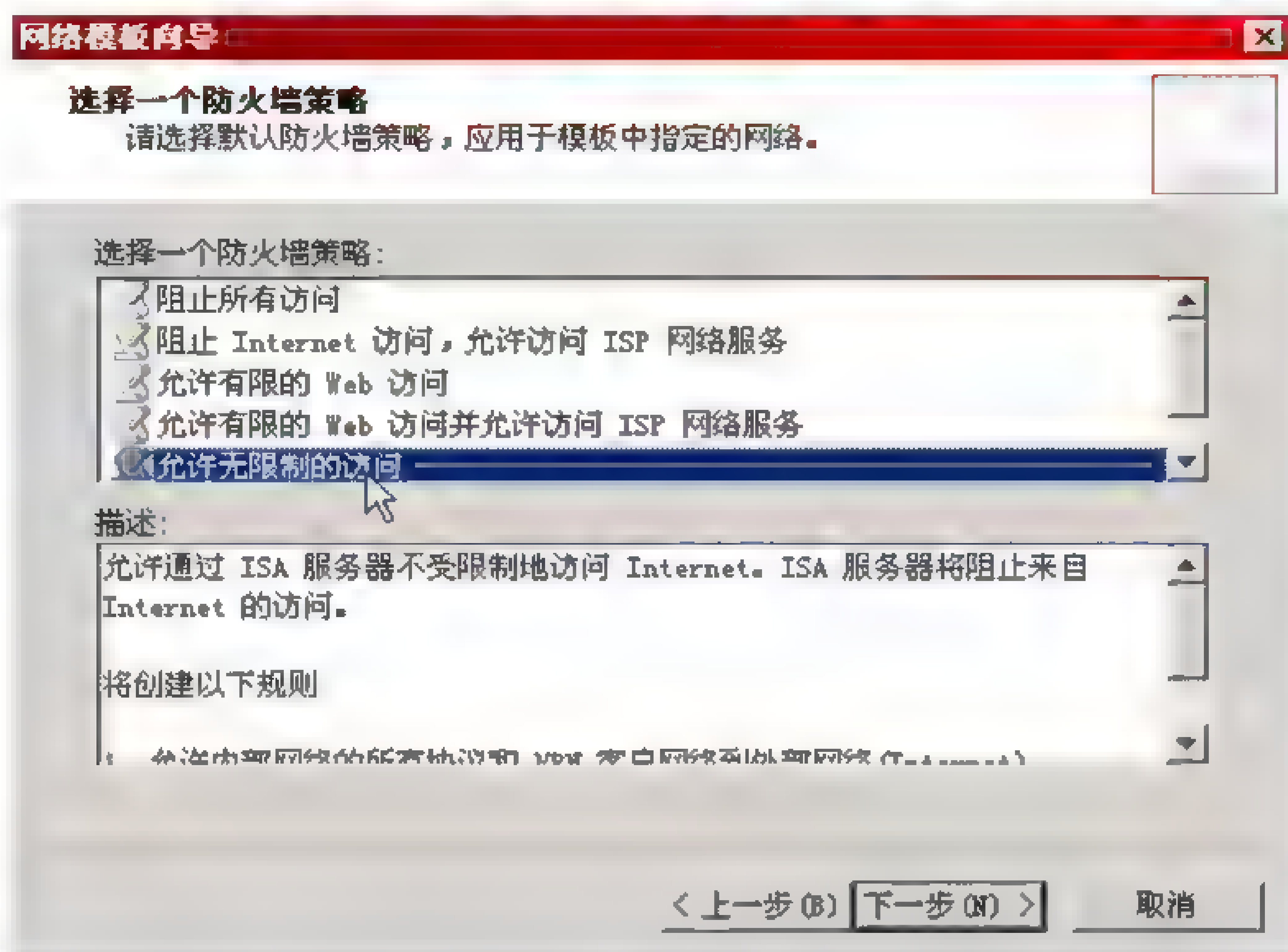


图 4-63　选择一个防火墙策略

（5）在“完成网络模板向导”对话框中单击“完成”按钮，此时，可以在防火墙策略看到新建的策略如图 4-64 所示。单击“应用”按钮保存修改和更新防火墙策略。



图 4-64　查看新建策略

（6）出于安全考虑，ISA Server 默认是不允许 FTP 上传的（即不能写 FTP 服务器）。取消的办法是：在允许访问 FTP 服务器的规则（在这里是“无限制的 Internet 访问”）上单击右键，从弹出的快捷菜单中选择“配置 FTP”命令。如图 4-65 所示。

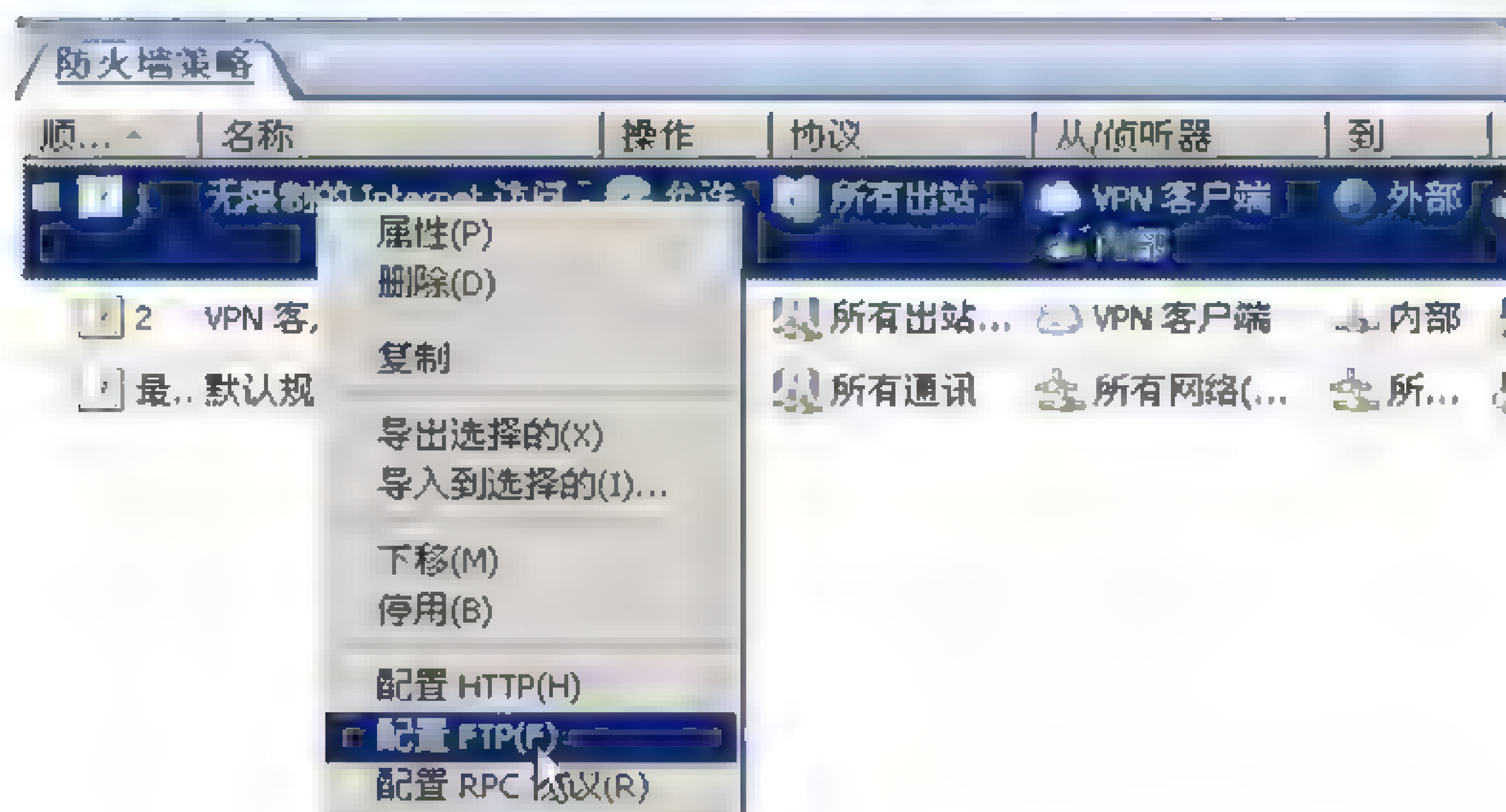


图 4-65 配置 FTP

（7）在图 4-66“配置 FTP 协议策略”对话框中，取消对“只读”复选框的勾选，单击“确定”按钮，最后单击“应用”按钮以保存修改和更新防火墙策略。

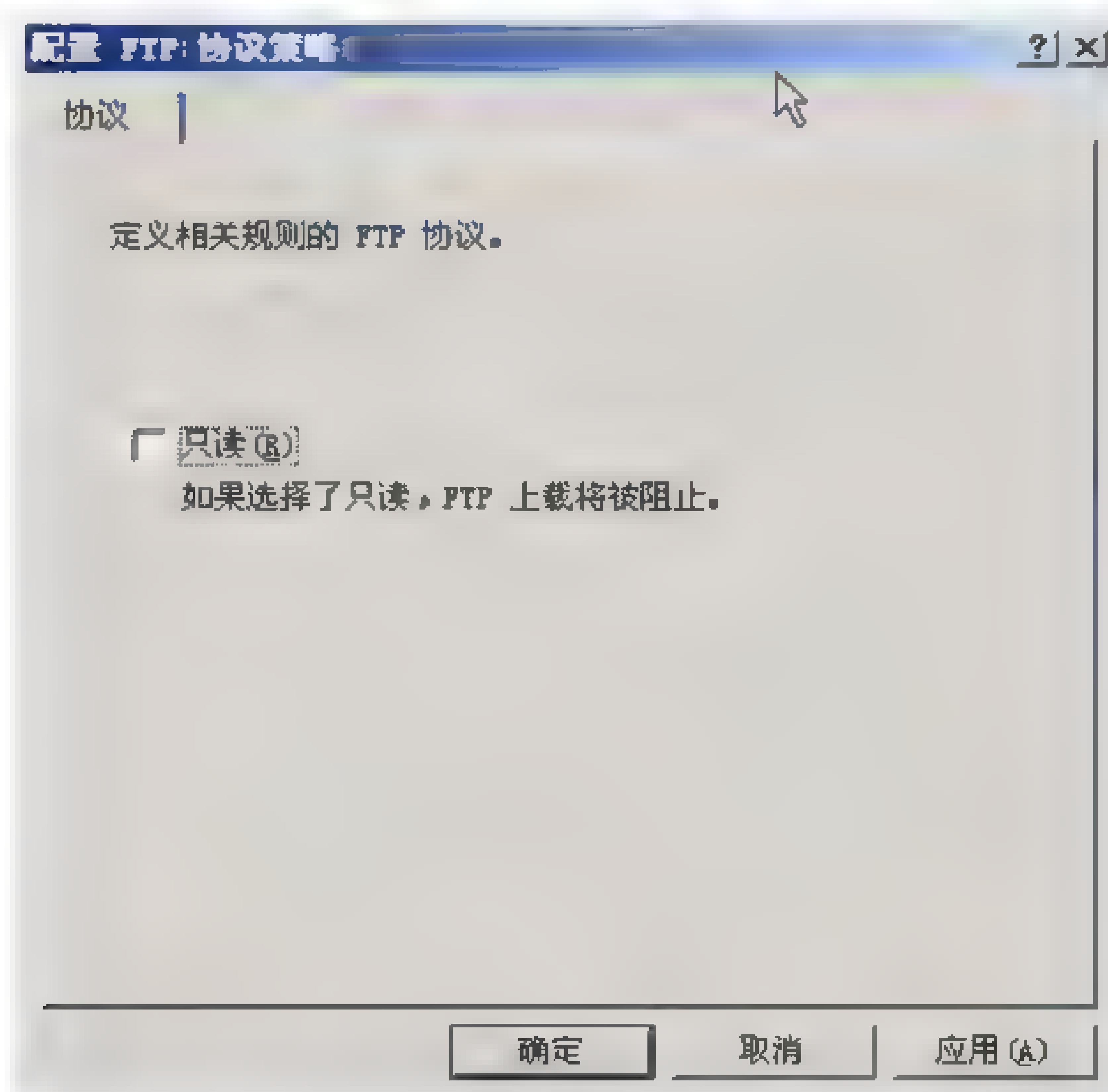


图 4-66 配置 FTP 协议策略

4.4.4 配置启用 HTTP 缓存

1. 设置缓存所用的驱动器

在 ISA Server 管理控制台的“缓存”上单击右键，从弹出的快捷菜单中选择“定义

缓存驱动器”命令。如图 4-67 所示，注意，此时的缓存上有个向下的红色箭头，表明没有启用缓存。

在图 4-68“定义缓存驱动器”对话框中，根据网络带宽及流量进行设置。

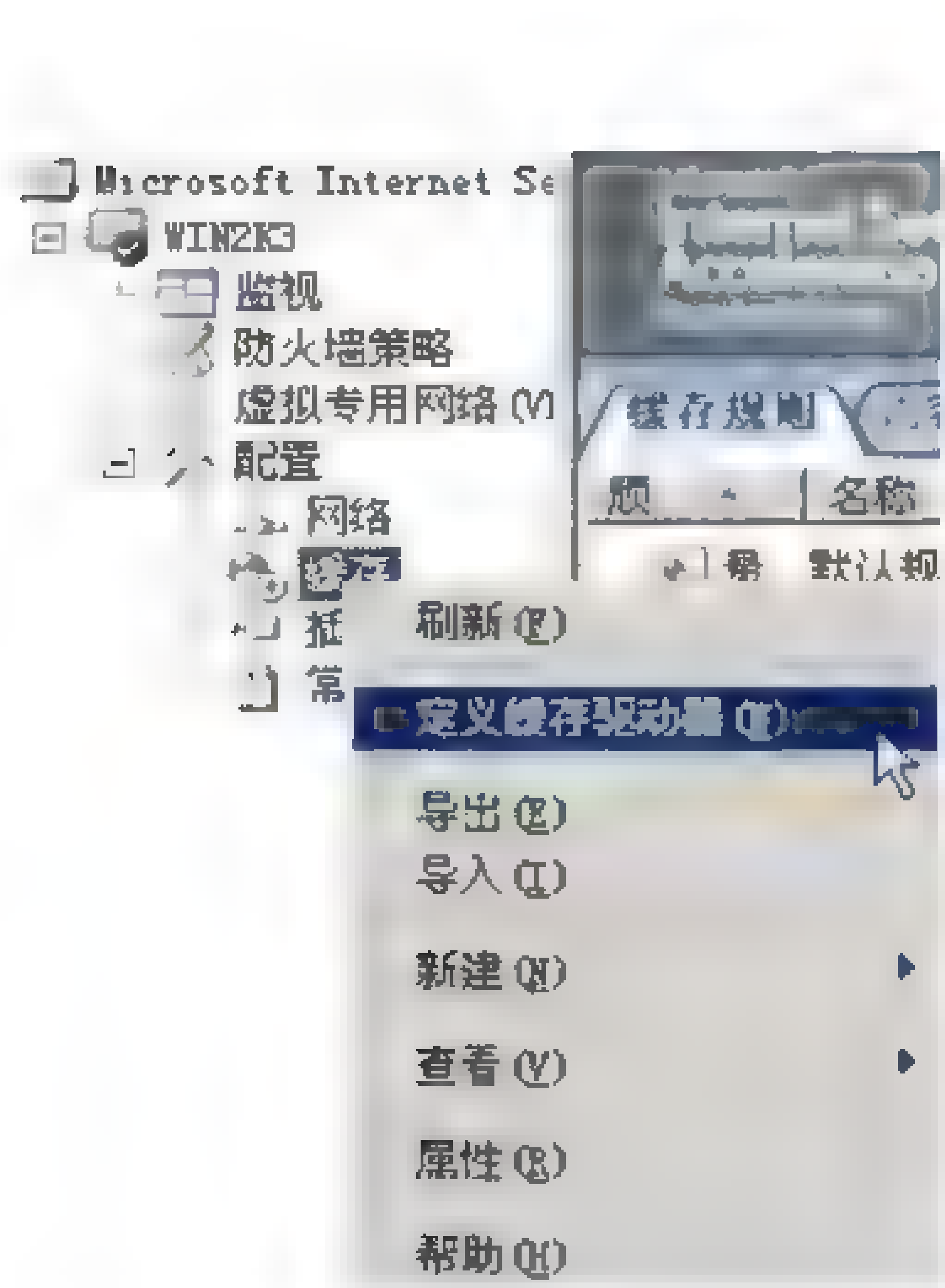


图 4-67　启动定义缓存驱动器

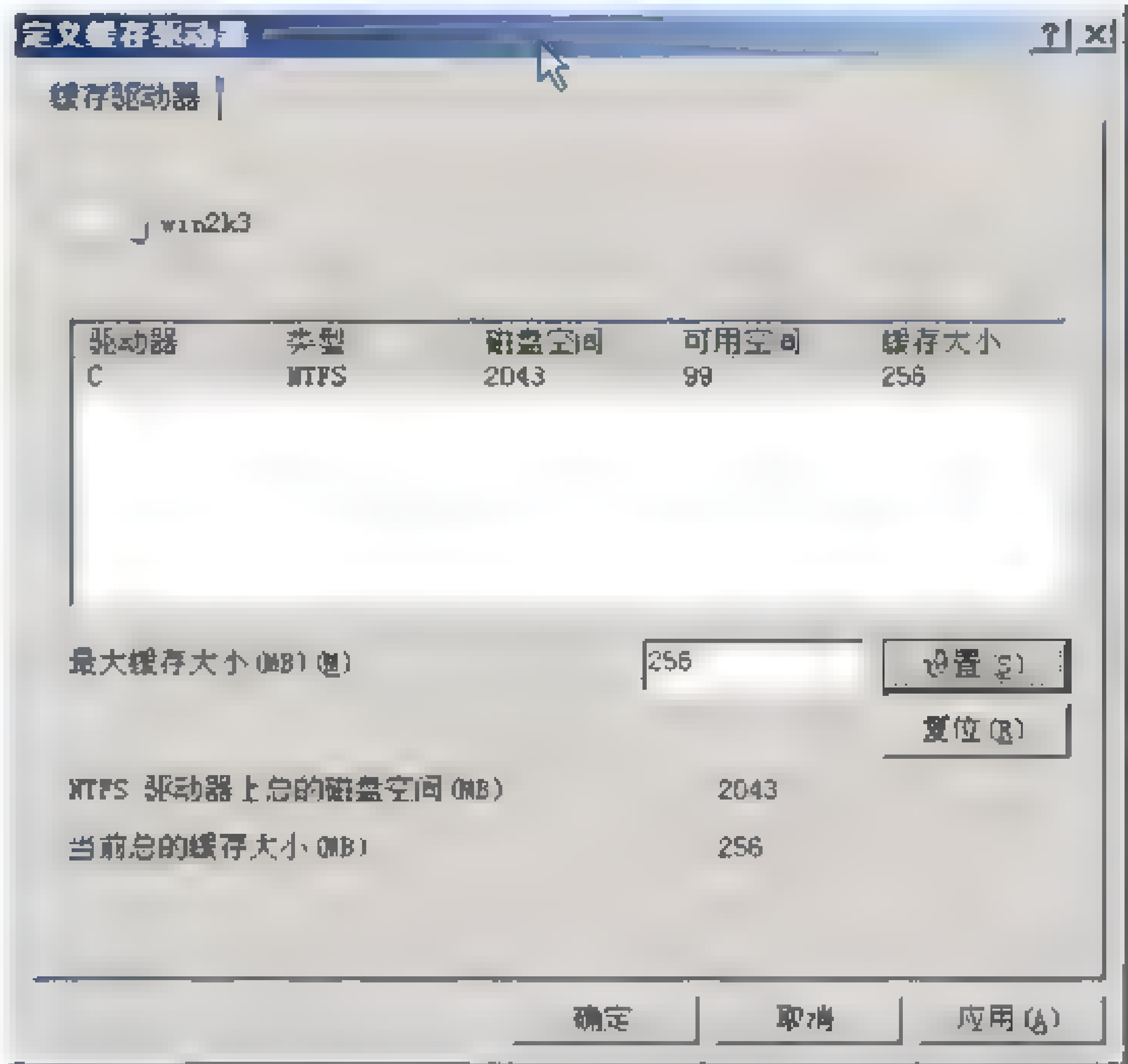


图 4-68　定义缓存驱动器

2. 设置缓存规则

此时“缓存”上已经没有向下的箭头了，表明已经设置了缓存驱动器。

（1）在“缓存”上单击右键，从弹出的快捷菜单中选择“新建”→“缓存规则”命令。如图 4-69 所示。

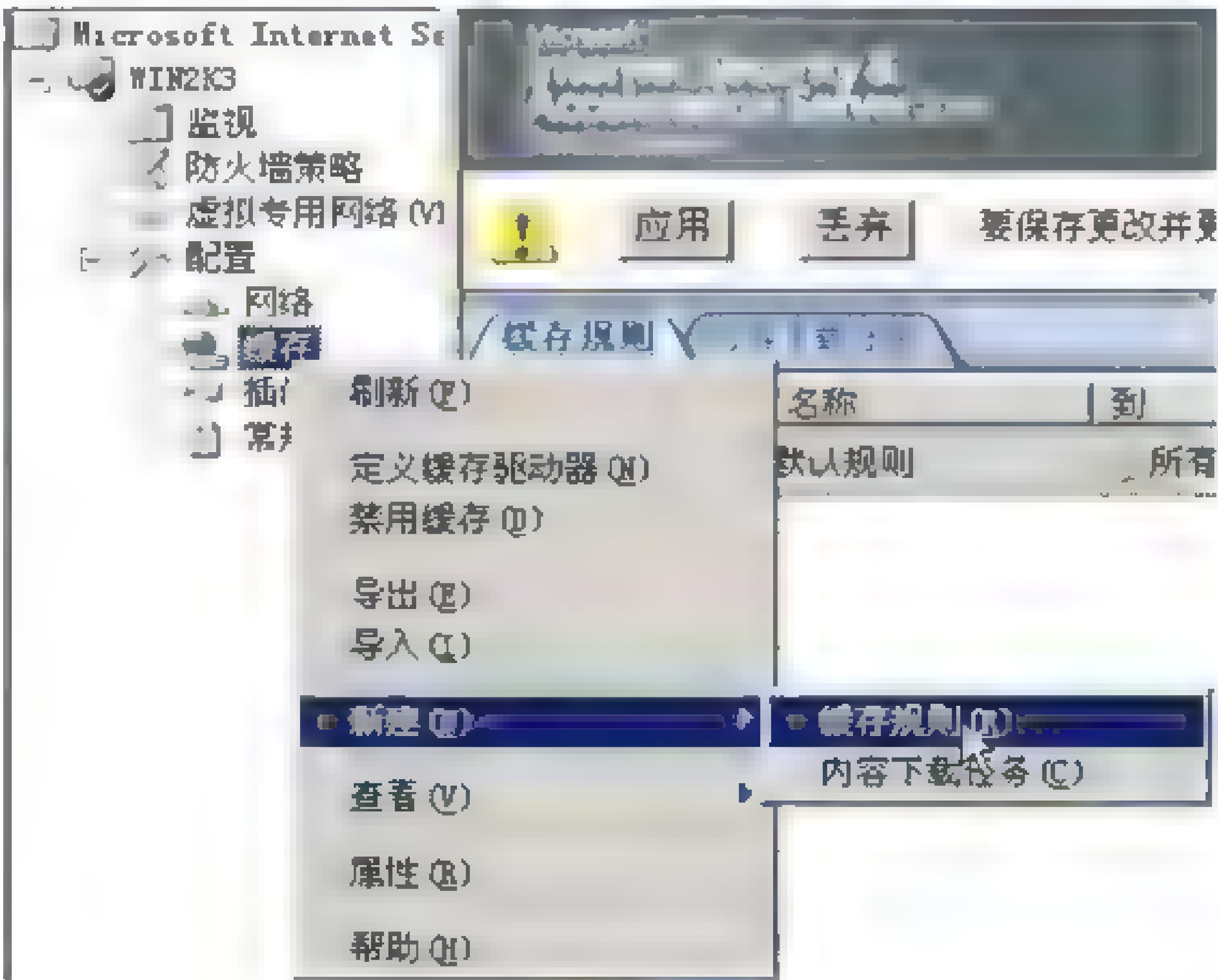


图 4-69　启动设置缓存规则

（2）在“新缓存规则向导”对话框中输入名称 Cache external content，然后单击“下一步”按钮。在“缓存规则目标”对话框中单击“添加”按钮，在打开的“添加网络实体”对话框中双击“外部”，单击“下一步”按钮。如图 4-70 所示。

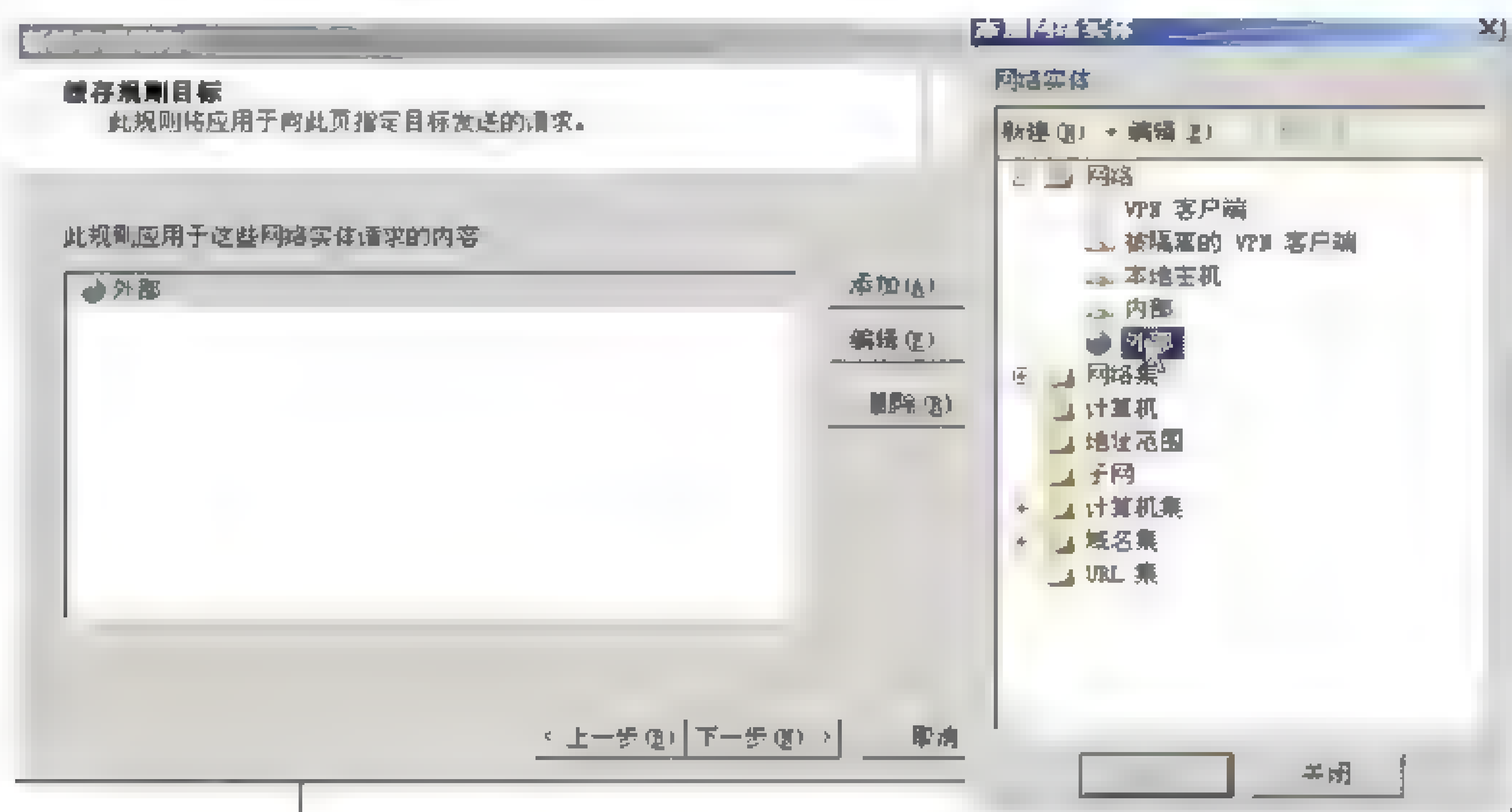


图 4-70　缓存规则目标

（3）在图 4-71“内容检索”对话框中，接受默认的“只有在缓存中存在对象的一个有效版本时。如果不存在有效版本，则传递请求到服务器。”单选按钮，单击“下一步”按钮。

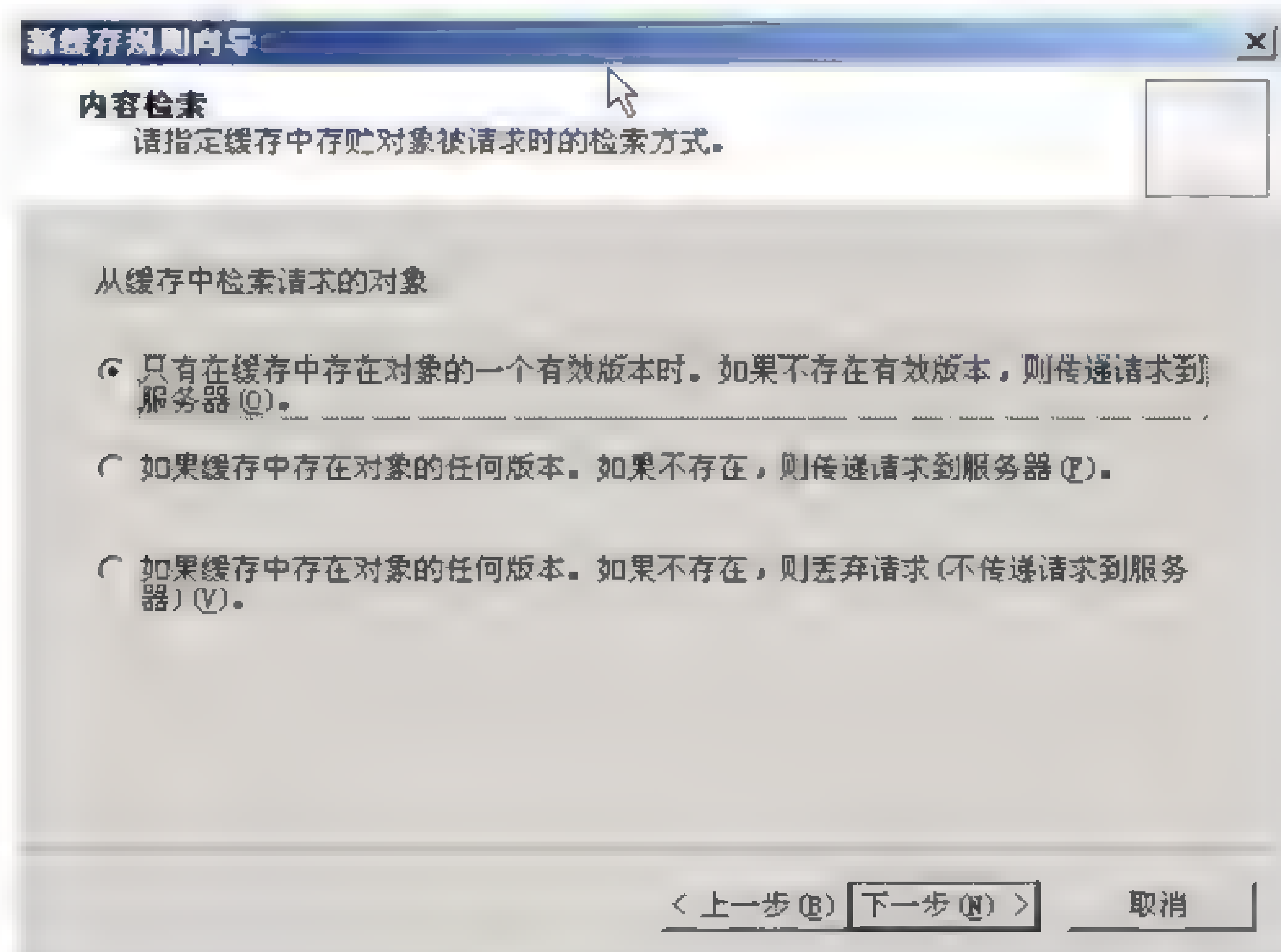


图 4-71　内容检索配置

（4）在图 4-72“缓存内容”对话框中，接受默认的“如果源和请求头指明要缓存”单选按钮，可以根据需要勾选下面的复选框，单击“下一步”按钮。

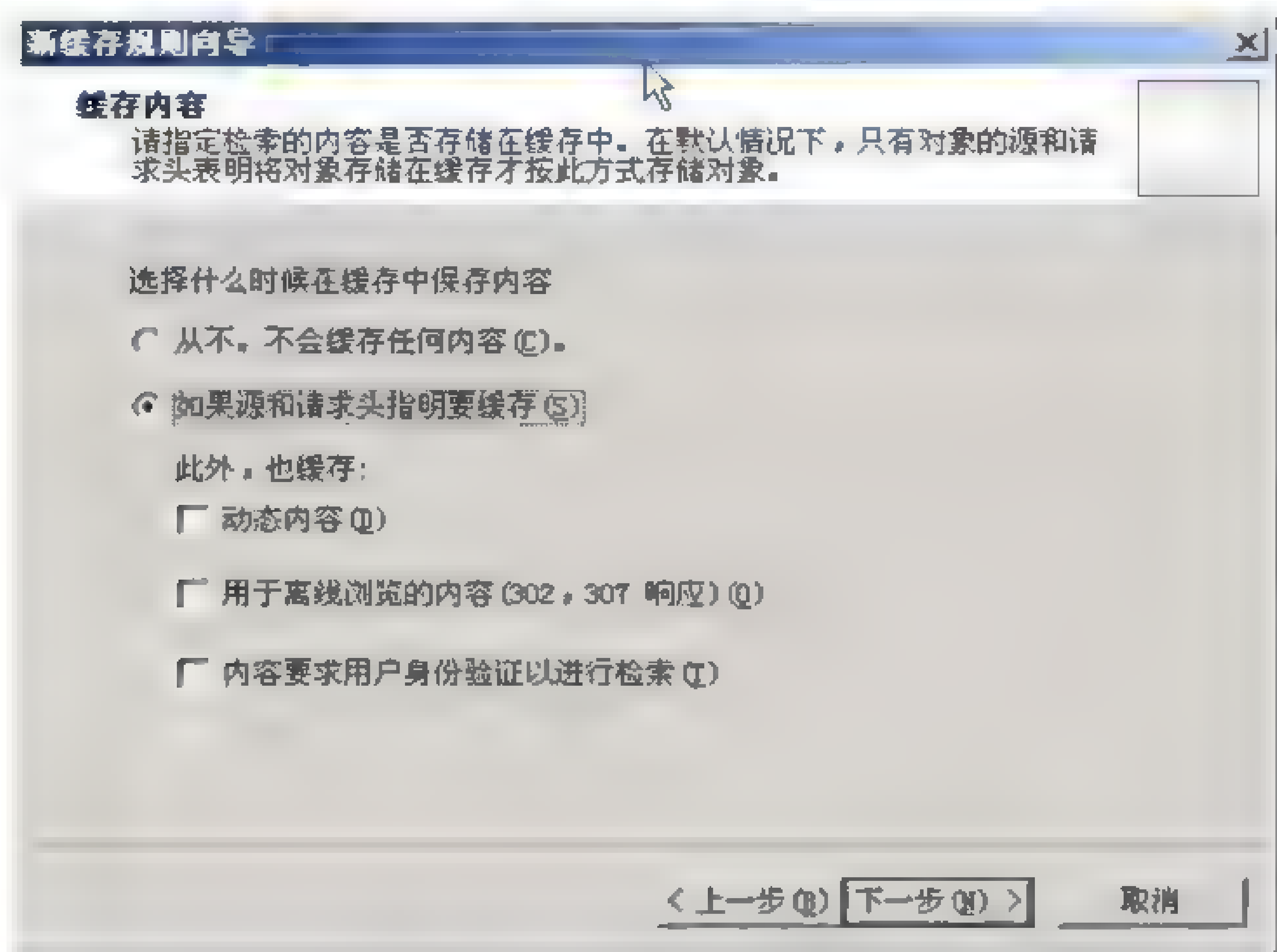


图 4-72　缓存内容配置

（5）在图 4-73“缓存高级配置”对话框中，根据需要进行设置，单击“下一步”按钮。

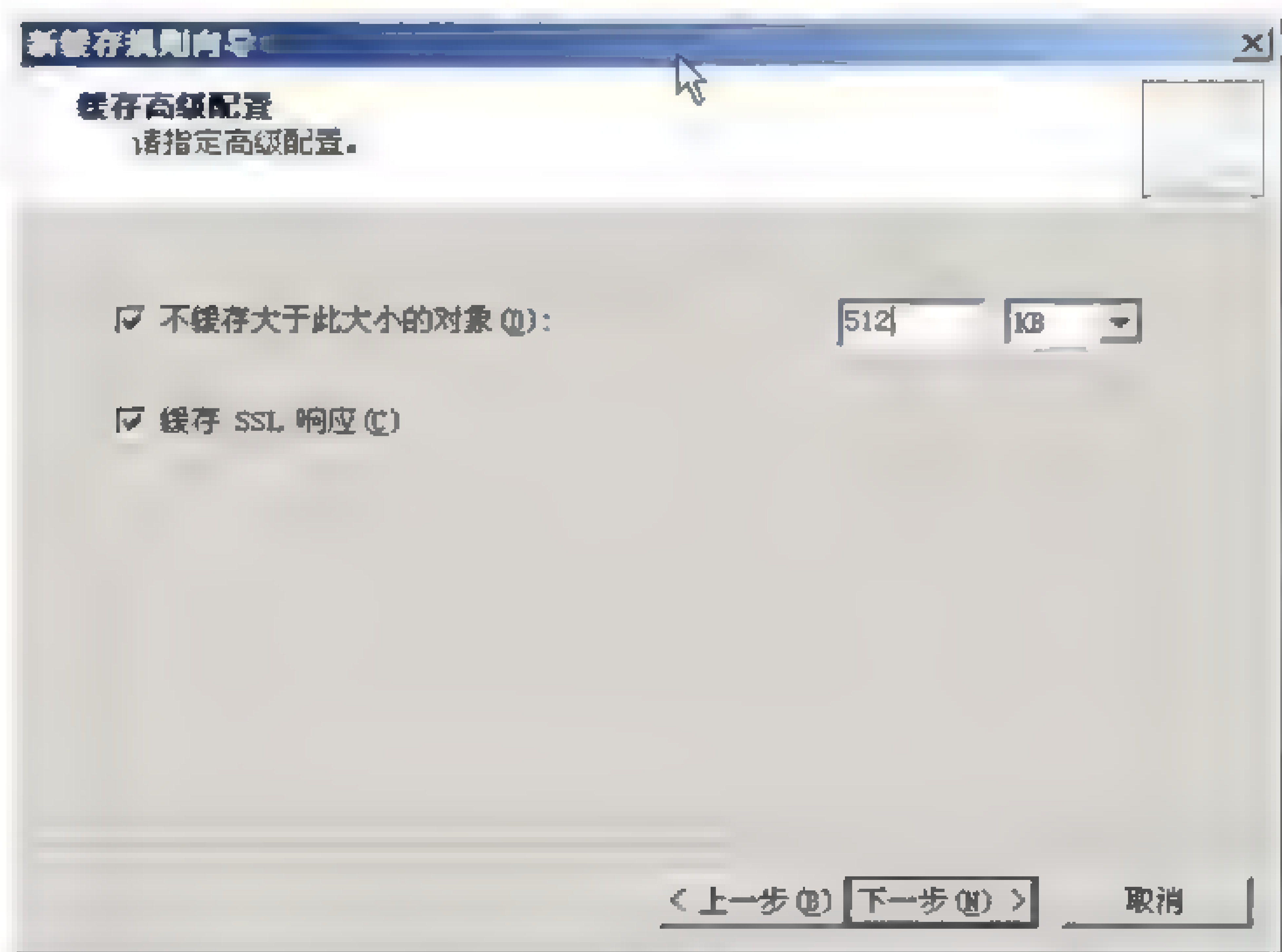


图 4-73　缓存高级配置

（6）在图 4-74“HTTP 缓存”对话框中，接受默认的选项，单击“下一步”按钮。

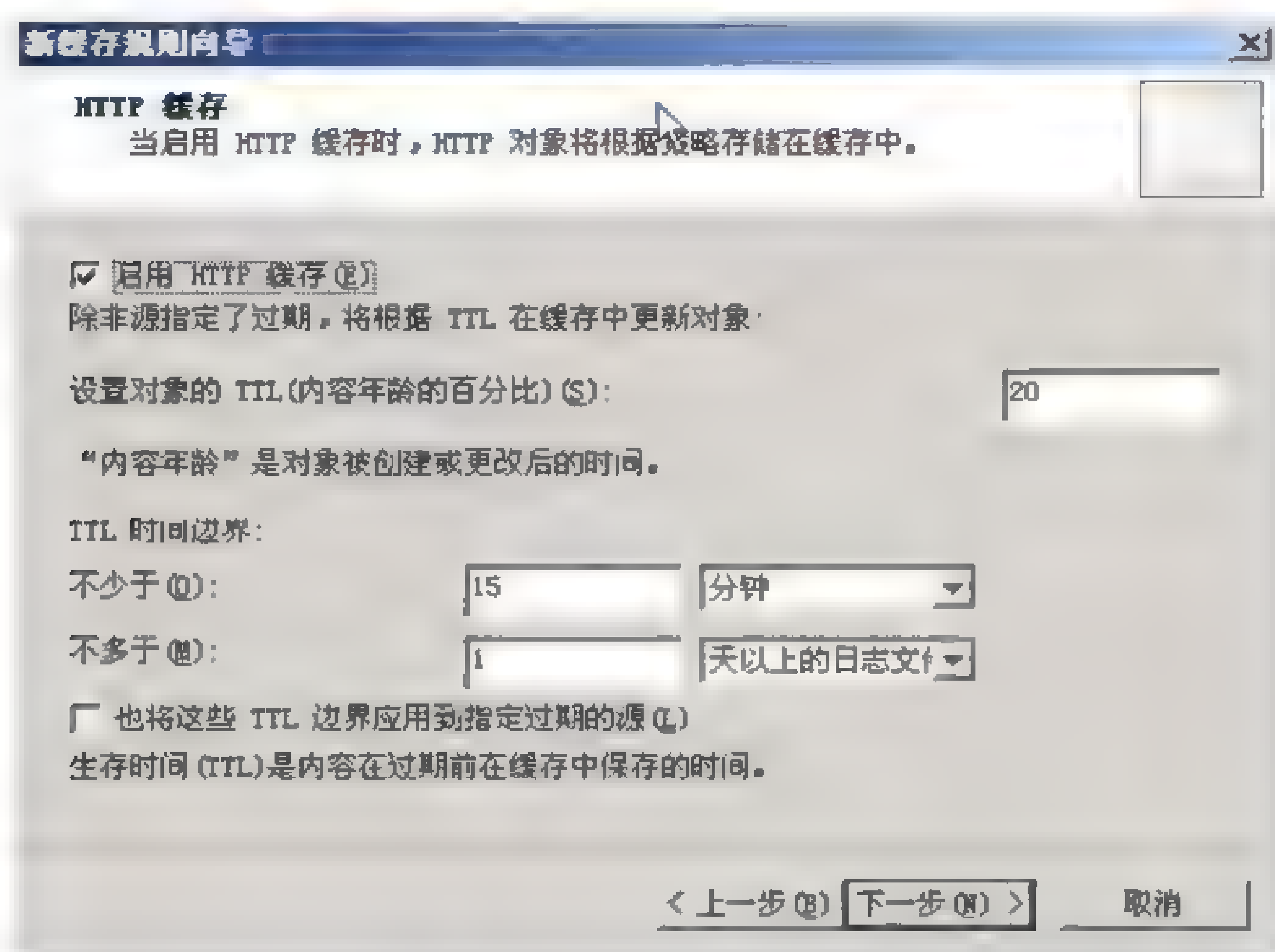


图 4-74　HTTP 缓存配置

（7）在图 4-75“FTP 缓存”对话框中，取消对“启用 FTP 缓存”复选框的勾选（可以根据需求进行设置），单击“下一步”按钮。

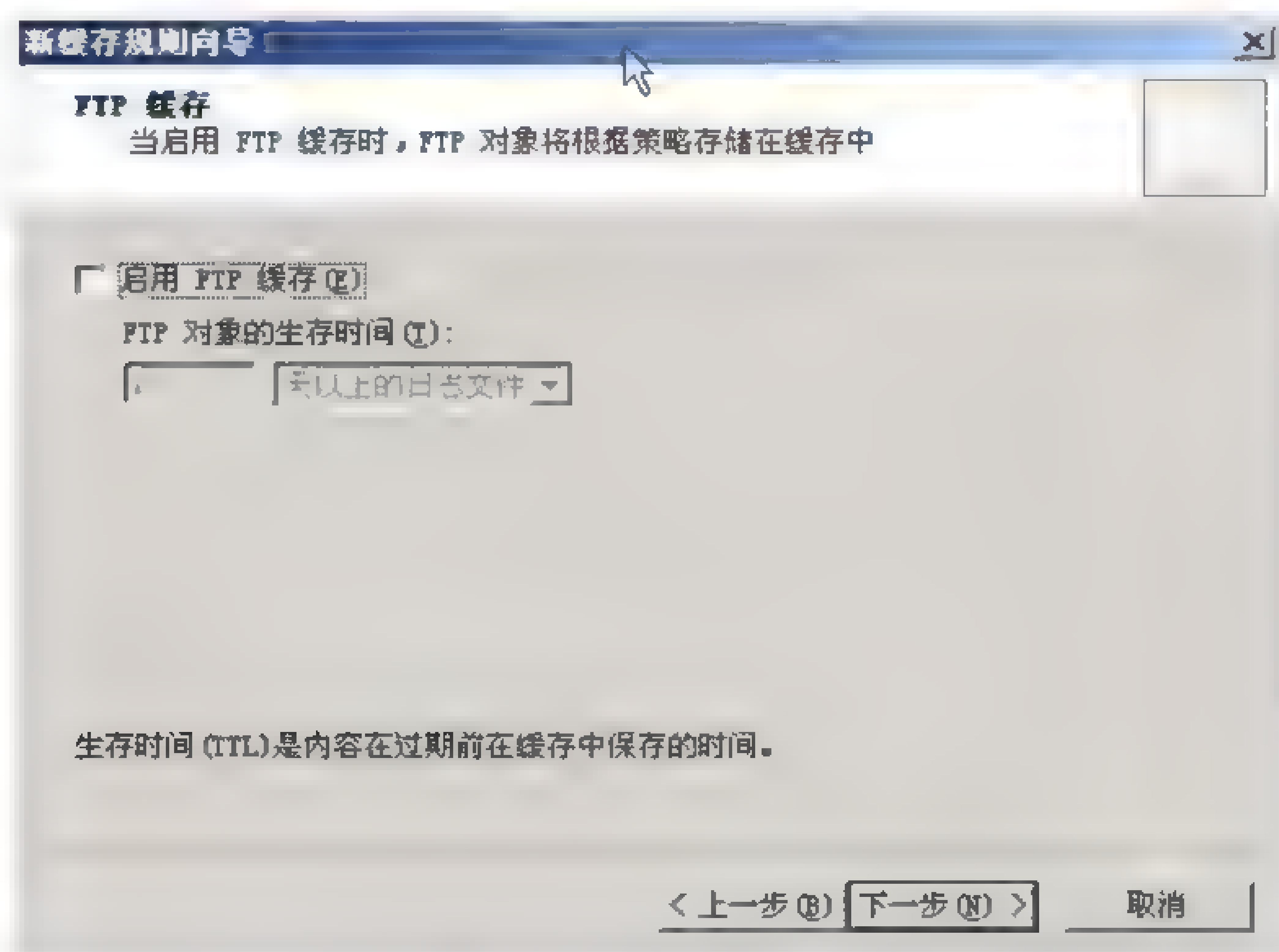


图 4-75　FTP 缓存配置

（8）在“完成新缓存规则向导”对话框中，回顾你的设置，然后单击“完成”按钮。

（9）单击“应用”按钮以保存修改和更新防火墙策略。ISA Server 2004 会弹出一个“ISA 服务器警告”对话框，选择“保存更改，并重启动服务”单选按钮，然后单击“确定”按钮。如图 4-76 所示。

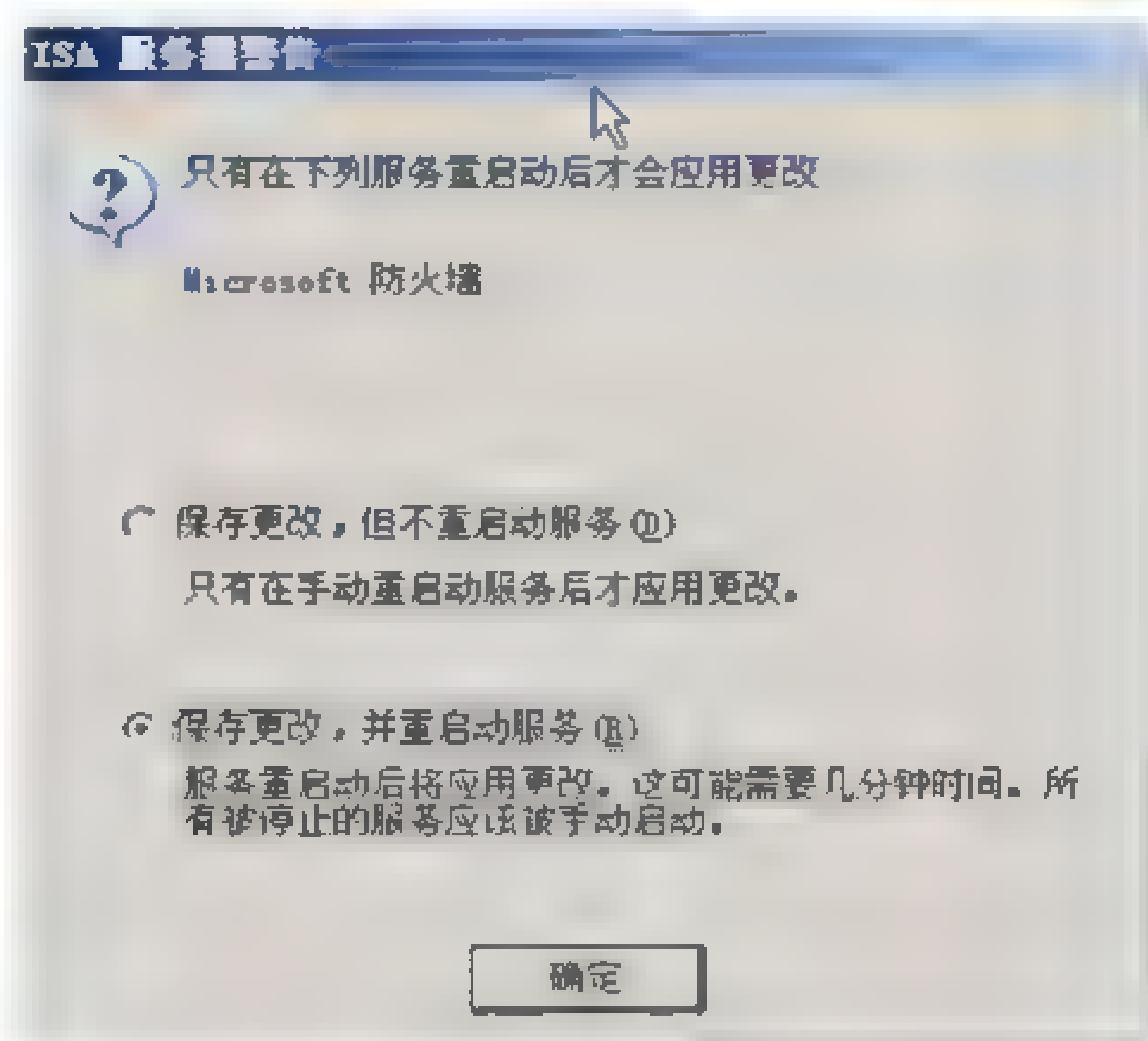


图 4-76　启动更改生效

成功后将在图 4-77“缓存规则”栏里面看见新的缓存规则。

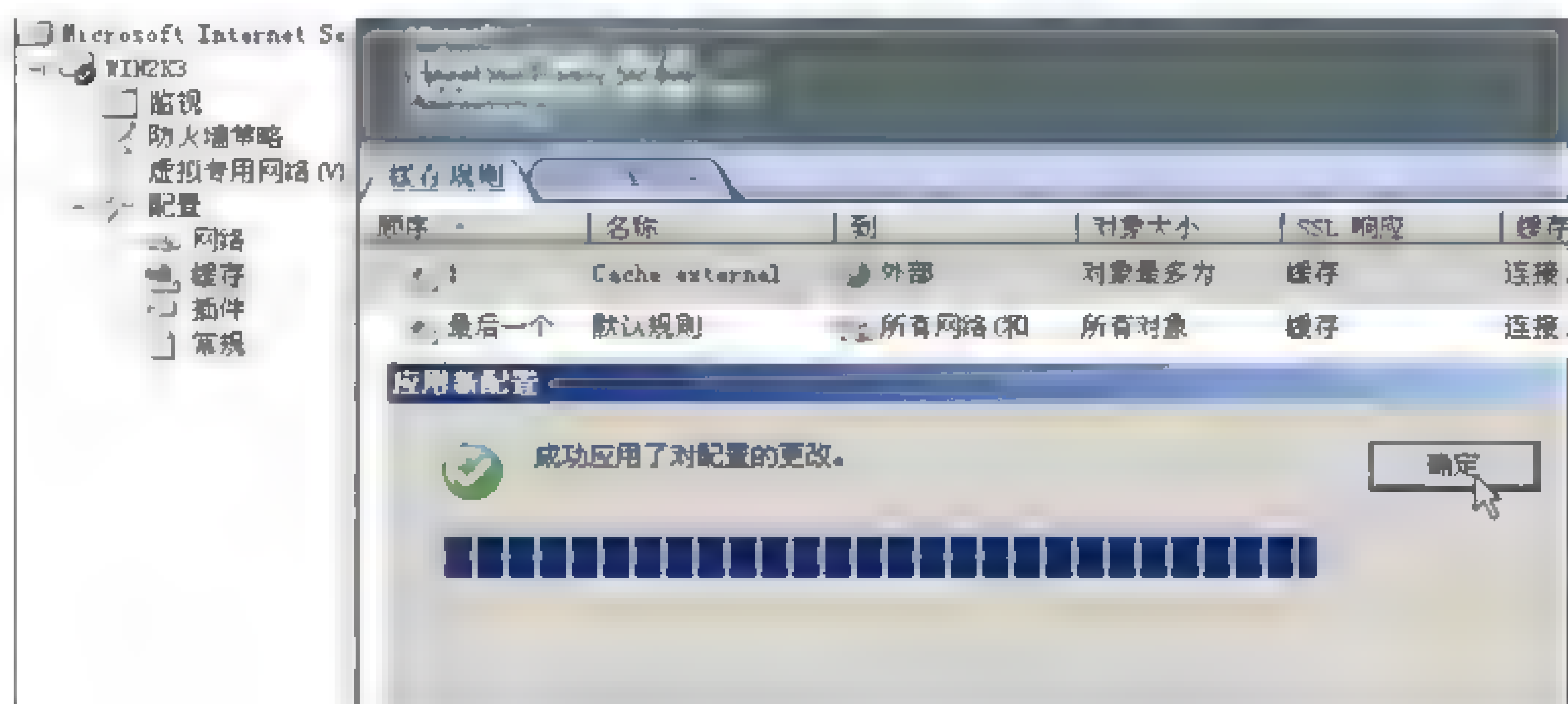


图 4-77　应用新配置

4.5　IDS 与 IPS

4.5.1　入侵检测系统概述

1．IDS 的定义

防火墙是阻止黑客攻击的一种有效手段，但随着攻击技术的发展，这种单一的防护

手段已不能确保网络的安全，它存在以下的弱点和不足。

（1）防火墙无法阻止内部人员所做的攻击。防火墙保护的是网络边界安全，对在网络内部所发生的攻击行为无能为力。而据调查，网络攻击事件有60%以上是由内部人员所为。

（2）防火墙对信息流的控制缺乏灵活性，防火墙是依据管理员定义的过滤规则对进出网络的信息流进行过滤和控制的。如果规则定义过于严格，则限制了网络的互连互通；如果规则定义过于宽松，则又带来了安全隐患。防火墙自身无法根据情况的变化进行自我调整。

（3）在攻击发生后，利用防火墙保存的信息难以调查和取证。而在攻击发生后，能够进行调查和取证，将罪犯绳之以法，是威慑网络罪犯、确保网络秩序的重要手段。防火墙由于自身的功能所限，难以识别复杂的网络攻击并保存相关的信息。

为了确保计算机网络安全，必须建立一整套的安全防护体系，进行多层次、多手段的检测和防护。入侵检测系统就是安全防护体系中重要的一环，它所具有的实时性、动态检测和主动防御等特点，弥补了防火墙等静态防御工具的不足，能够及时识别网络中发生的入侵行为并实时报警。

入侵检测系统（Intrusion Detection System，IDS）是一种主动保护自己，使网络和系统免遭非法攻击的网络安全技术，它依照一定的安全策略，对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或攻击结果，以保证网络系统资源的机密性、完整性和可用性。

入侵检测系统是对防火墙的一个极其有益的补充，我们做一个形象的比喻：假如防火墙是一栋大楼的门锁，那么IDS就是这栋大楼里的监视系统。一旦小偷爬窗进入大楼，或者内部人员有越界行为，只有实时监视系统才能发现情况并发出警告。

2．IDS的作用

入侵检测系统作为一种积极主动的安全防护工具，提供了对内部攻击、外部攻击和误操作的实时防护，在计算机网络和系统受到危害之前进行报警、拦截和响应。它具有以下主要作用。

（1）通过检测和记录网络中的安全违规行为，惩罚网络犯罪，防止网络入侵事件的发生。

（2）检测其他安全措施未能阻止的攻击或安全违规行为。

（3）检测黑客在攻击前的探测行为，预先给管理员发出警报。

（4）报告计算机系统或网络中存在的安全威胁。

（5）提供有关攻击的信息，帮助管理员诊断网络中存在的安全弱点，利于其进行修补。

（6）在大型、复杂的计算机网络中布置入侵检测系统，可以显著提高网络安全管理的质量。

3. IDS 的组成

一个 IDS 系统通常由探测器（Sensor）、分析器（Analyzer）、响应单元（Response Units）和事件数据库（Event Databases）组成。

事件是 IDS 中所分析的数据的统称，它可以是从系统日志、应用程序日志中所产生的信息，也可以是在网络中抓到的数据包。

（1）探测器。探测器主要负责收集数据。入侵检测的第一步就是收集数据，内容包括任何可能包含入侵行为线索的系统数据，如网络数据包、日志文件和系统调用记录等。通常需要在计算机网络系统中的若干个不同的关键点（不同网段和不同主机）收集数据，这是因为入侵检测在很大程度上依赖于收集数据的正确性和可靠性。有时从一个数据源来的数据有可能看不出问题，但是从几个数据源来的数据的不一致却是可疑行为或入侵的最好标识。探测器将这些数据收集起来后，发送到分析器进行处理。

（2）分析器。又称分析部件，它的作用是分析从探测器中获得的数据，主要包括两个方面：一是监控进出主机和网络的数据流，看是否存在对系统的入侵行为；另一个是评估系统关键资源和数据文件的完整性，看系统是否已经遭受了入侵。前者的作用是在入侵行为发生时发现它，从而避免遭受攻击；后者是在遭受攻击时未能及时发现和阻止攻击行为，但可以通过攻击行为留下的痕迹了解攻击行为的一些情况，从而避免再次遭受攻击。对系统资源完整性的检查也有利于对攻击行为进行取证。

（3）响应单元。又称控制台部件，它的作用是对分析所得结果做出相应的动作，或者是报警，或者是更改文件属性，或者是阻断网络连接等。

（4）事件数据库。又称日志部件，存放的是各种中间数据，记录攻击的基本情况。

4. IDS 的类型及技术

1）根据数据来源和系统结构的不同，入侵检测系统可以分为基于主机、基于网络和混合性入侵检测系统三类

（1）基于主机的入侵检测（Host-based Intrusion Detection System，HIDS）通常在被重点检测的主机上运行一个代理程序，用于监视、检测对于主机的攻击行为（如可疑的网络连接、系统日志检查和非法访问等），通知用户并进行响应。HID 最适合配置来对抗内部的威胁，因为它能监视并响应用户特殊的行为以及对主机文件的访问行为。因此，它保护的一般是所在的系统。由于这种类型的系统依赖于审计数据或系统日志的准确性和完整性以及安全事件的定义，所以若入侵者设法逃避审计或进行合作入侵，则基于主机的检测系统就会暴露出弱点，特别是在现在的网络环境下，单独依靠主机审计信息进行入侵检测已难以适应网络安全的需要。

（2）基于网络的入侵检测（Network Intrusion Detection System，NIDS）数据源是网络上的数据包，在这种类型的入侵检测系统中，往往将一台机器的网卡设置于混杂模式，监听所有本网段内的数据包并进行判断。一般网络型入侵检测系统担负着保护整个网段的任务。它不停地监视网段中的各种数据包，对每一个可疑的数据包进行特征分析：如果数据包与内置的某些规则吻合，入侵检测系统就会发出警报甚至直接切断网络连接。

目前，大部分入侵检测产品是基于网络的。基于网络的 IDS 易于配置和易于作为一个独立的组件来进行管理，而且它们对受保护系统的性能也不产生影响或影响很小。在网络入侵检测系统中，有多个久负盛名的开放源码软件，如 Snort、NFR 和 Shadow 等。图 4-78 是一个典型的基于网络的入侵检测系统的模型。

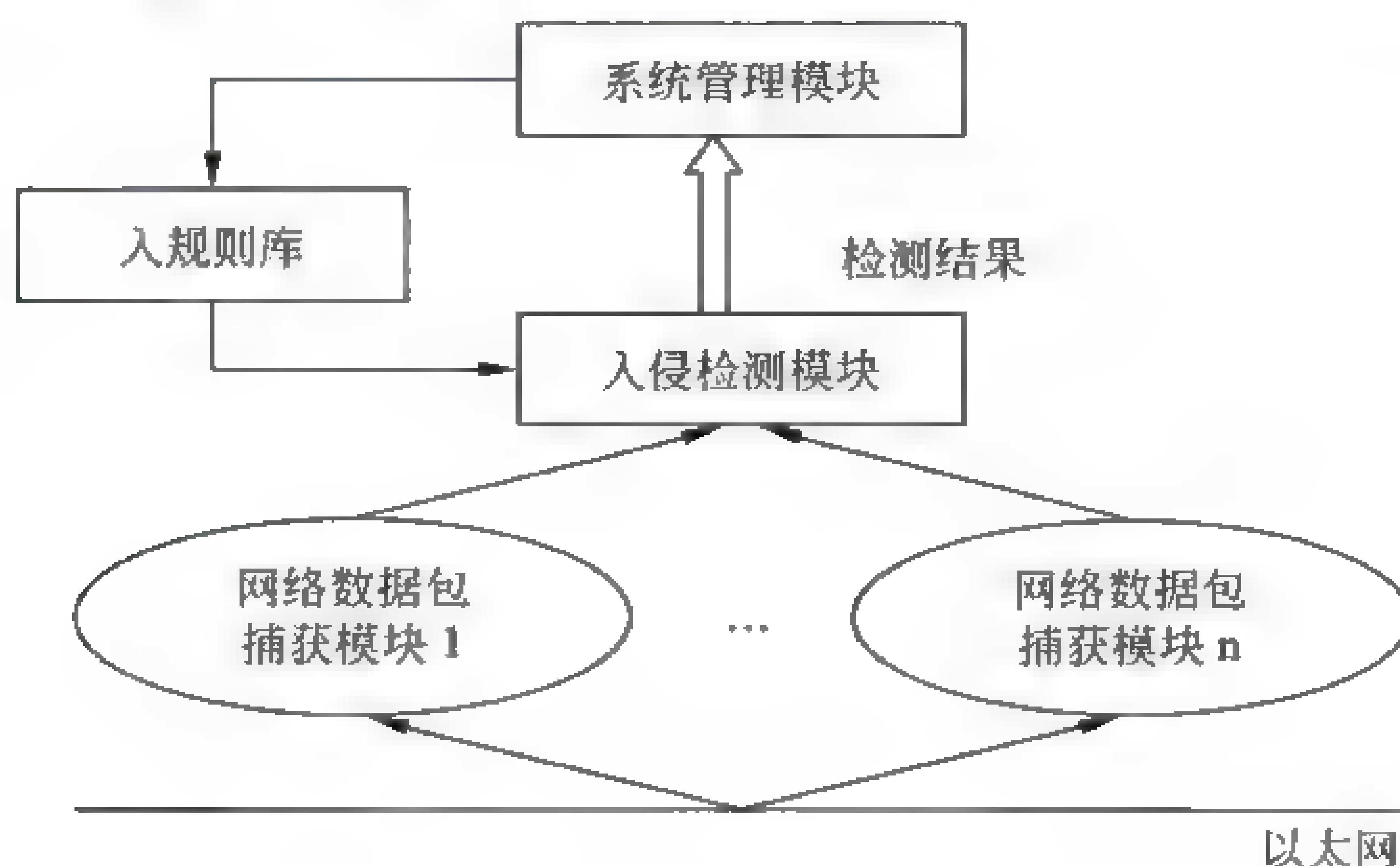


图 4-78 NIDS 模型

（3）混合型是基于主机和基于网络的入侵检测系统的结合，它为前两种方案提供了互补，还提供了入侵检测的集中管理，采用这种技术能实现对入侵行为的全方位检测。

2）根据入侵检测所采用的技术，可以分为异常检测和误用检测两类

（1）异常检测（Abnormal Detection）。能够根据异常行为和使用计算机资源的情况检测出入侵。该技术通过流量统计分析建立系统正常行为的轨迹，当系统运行时的数值超过正常阈值则认为可能受到攻击，其技术本身就导致了漏报误报率较高。

（2）误用检测（Misuse Detection）。该技术是建立在使用某种模式或者特征描述方法能够对任何已知攻击进行表达这一理论基础上的，其关键是如何正确表达入侵的模式，把真正的入侵与正常行为区分开来。误用检测可以直接识别攻击，误报率低。缺点是只能检测已定义的攻击方法，对新的攻击方法无能为力，必须及时更新模式库。

通常 IDS 将这两种检测技术相结合，像 Cisco 公司的 ID 就是这种解决方案的一个实例。它首先检查特征库，如果有特征匹配，则采用基于模式匹配或基于签名的方法检测入侵；如果没有特征匹配，就采用基于异常统计的方法检测入侵。

5．分布式入侵检测系统

传统的集中式 IDS 的基本模型是在网络的不同网段放置多个探测器收集当前网络状态的信息，然后将这些信息传送到中央控制台进行分析处理。这种方式存在明显的缺陷。

（1）对于大规模分布式攻击，中央控制台的负荷将会超过其处理极限，这种情况会造成大量信息处理的遗漏，导致漏警率的增高。

（2）多个探测器收集到的数据在网络上的传输会在一定程度上增加网络负担，导致

网络系统性能的降低。

（3）由于网络传输的时延问题，中央控制台处理的网络数据包中所包含的信息只反应了探测器接受到它时网络的状态，不能实时反应当前网络状态。

现代 IDS 必须能够实现局部实时检测，全局信息共享，只有这样才能够有效应对现代网络的特点。因此，分布式入侵检测系统（Distributed Intrusion Detection System，DIDS）应运而生。DIDS 采用了分布式智能代理的结构方式，由几个中央智能代理和大量分布的本地代理组成，其中本地代理负责处理本地事件，而中央代理负责整体的分析工作。与集中式模型不同，它强调的是通过全体智能代理协同工作来分析入侵者的攻击策略，中央代理扮演的是协调者和全局分析员的角色，但绝对不是唯一的事件处理者，其地位就像是战场上的元帅，根据对全局形式的判断指挥部下开展行动。本地代理有较强的自主性，可以独立对本地攻击进行有效的检测。同时，它也和中央智能代理和其他本地代理通信，接受中央代理的调度指挥并与其他代理协同工作。

一个简单的分布式入侵检测系统如图 4-79 所示。

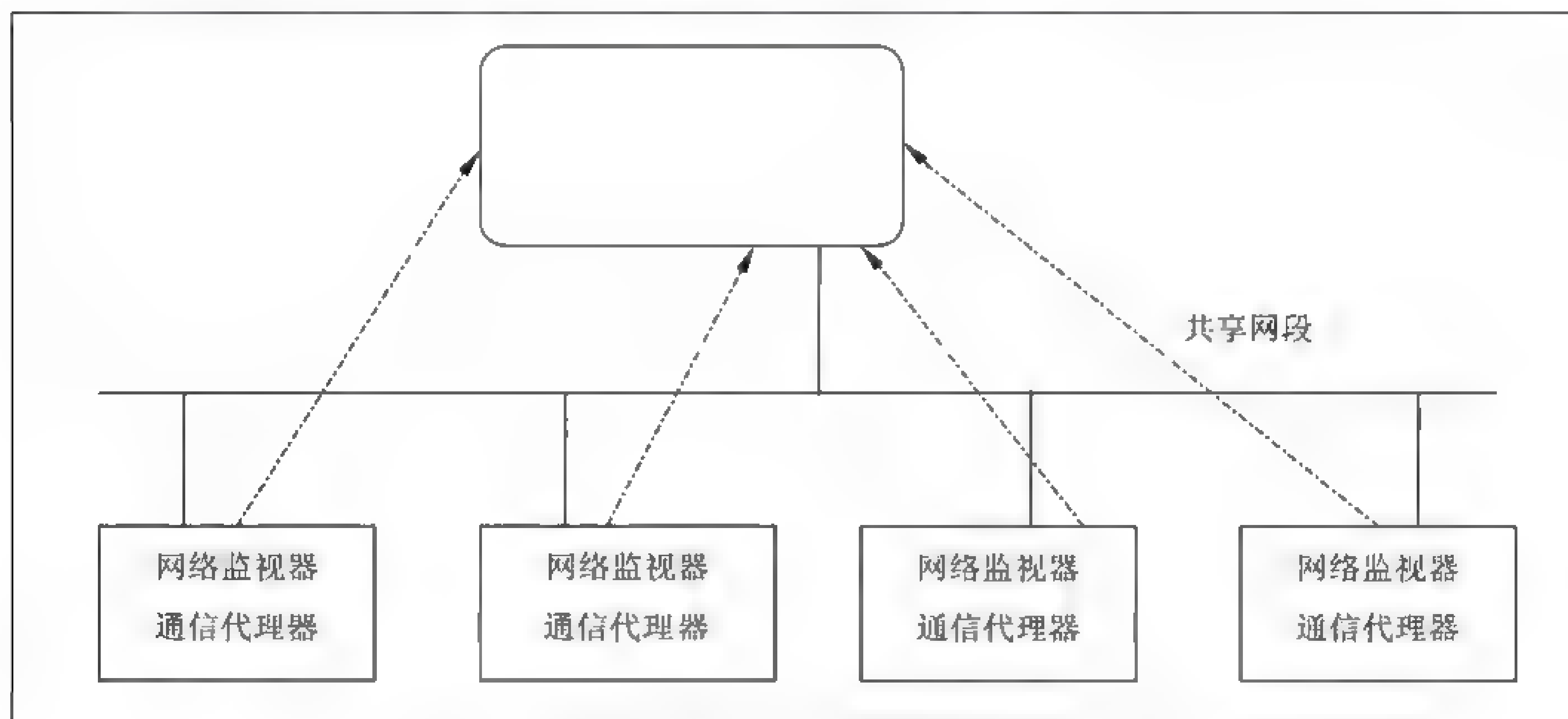


图 4-79 DIDS 系统

- 用户接口：主要负责给安全管理者提供友好的人机界面。
- 通信代理器：主要负责控制整个系统的信息流。
- 网络监视器：主要负责监视网络中的数据，通过通信代理模块向 DIDS 中央控制台发送信息。

4.5.2 入侵检测系统实例

1．RIDS-100

RIDS-100 入侵检测系统是由瑞星公司自主开发研制的新一代网络安全产品，它集入

侵检测、网络管理和网络监视功能于一身，能实时捕获内外网之间传输的所有数据，利用内置的攻击特征库，使用模式匹配和智能分析的方法，检测网络上发生的入侵行为和异常现象，并在数据库中记录有关事件，作为管理员事后分析的依据。如果情况严重，RIDS-100 可以发出实时报警，使得管理员能够及时采取应对措施。

RIDS-100 入侵检测系统是一套基于网络的分布式入侵检测系统，它主要由入侵检测引擎和管理控制台两部分组成，如图 4-80 所示。

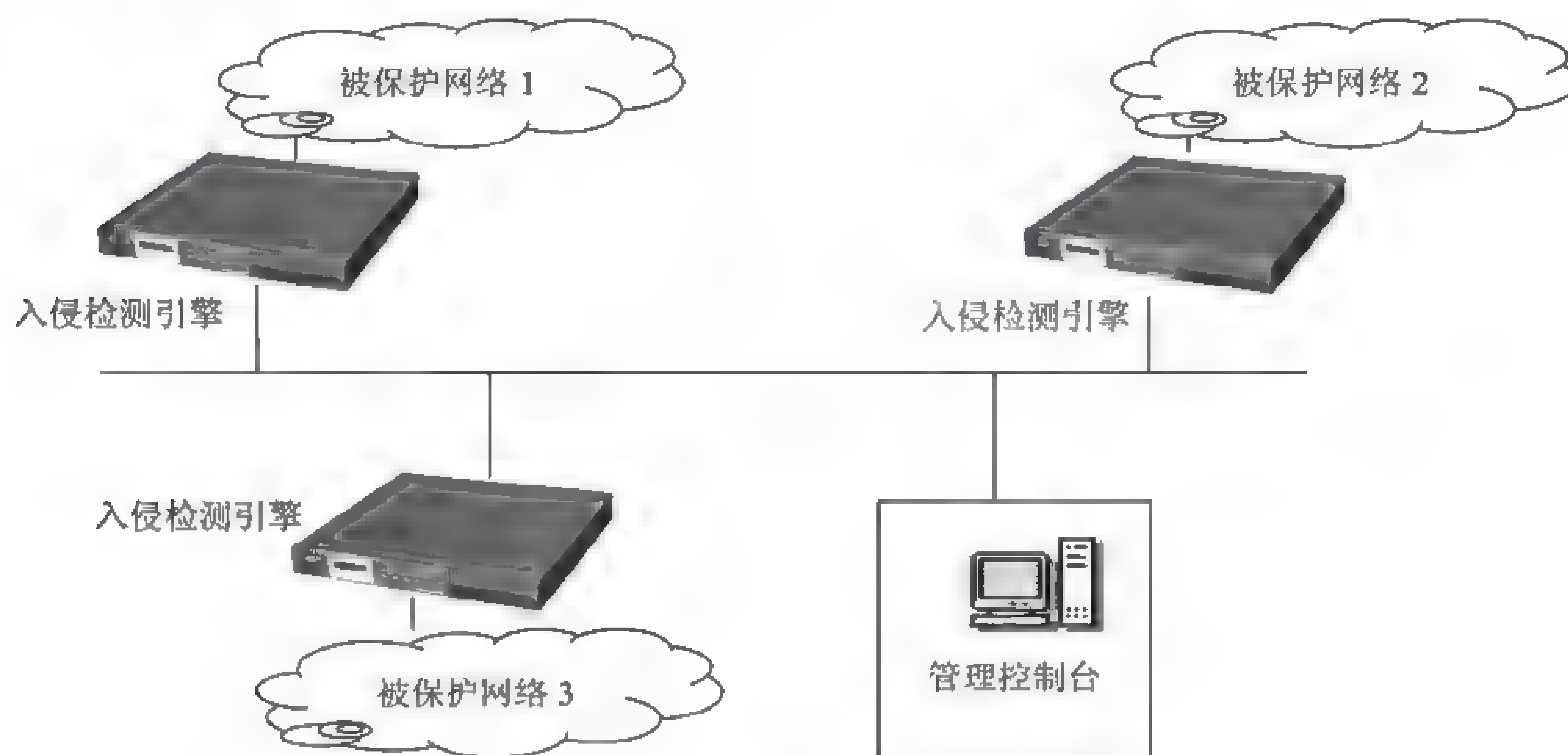


图 4-80 入侵检测系统组成图

1）入侵检测引擎

入侵检测引擎为专用硬件设备（如图 4-81 所示），可以安装在标准的机架上，一个检测引擎可以保护一个网段。



图 4-81 RIDS-100 入侵检测引擎

检测引擎有两个以太网接口：数据捕获口和查询管理口。

检测引擎的数据捕获口接在被保护网段上，它以隐身模式从网络线路上获取数据，然后调用相应的处理模块进行分析处理，如果发现异常事件，则调用告警器，由其根据预定义的处理规则，决定调用相应的响应模块。响应模块可以采取多种手段向系统管理

员或被攻击主机报警，也可以主动切断发生攻击的连接。

查询管理口接在管理主机可以访问的网络上，它是管理控制台和引擎进行通信的接口。

检测引擎采用模块化设计结构（如图 4-82 所示），具有很好的可扩展性。引擎包含的功能模块有包捕获模块、虚拟机模块、攻击特征库、过滤器模块、智能分析模块、记录器模块、报警模块和磁盘管理模块等。

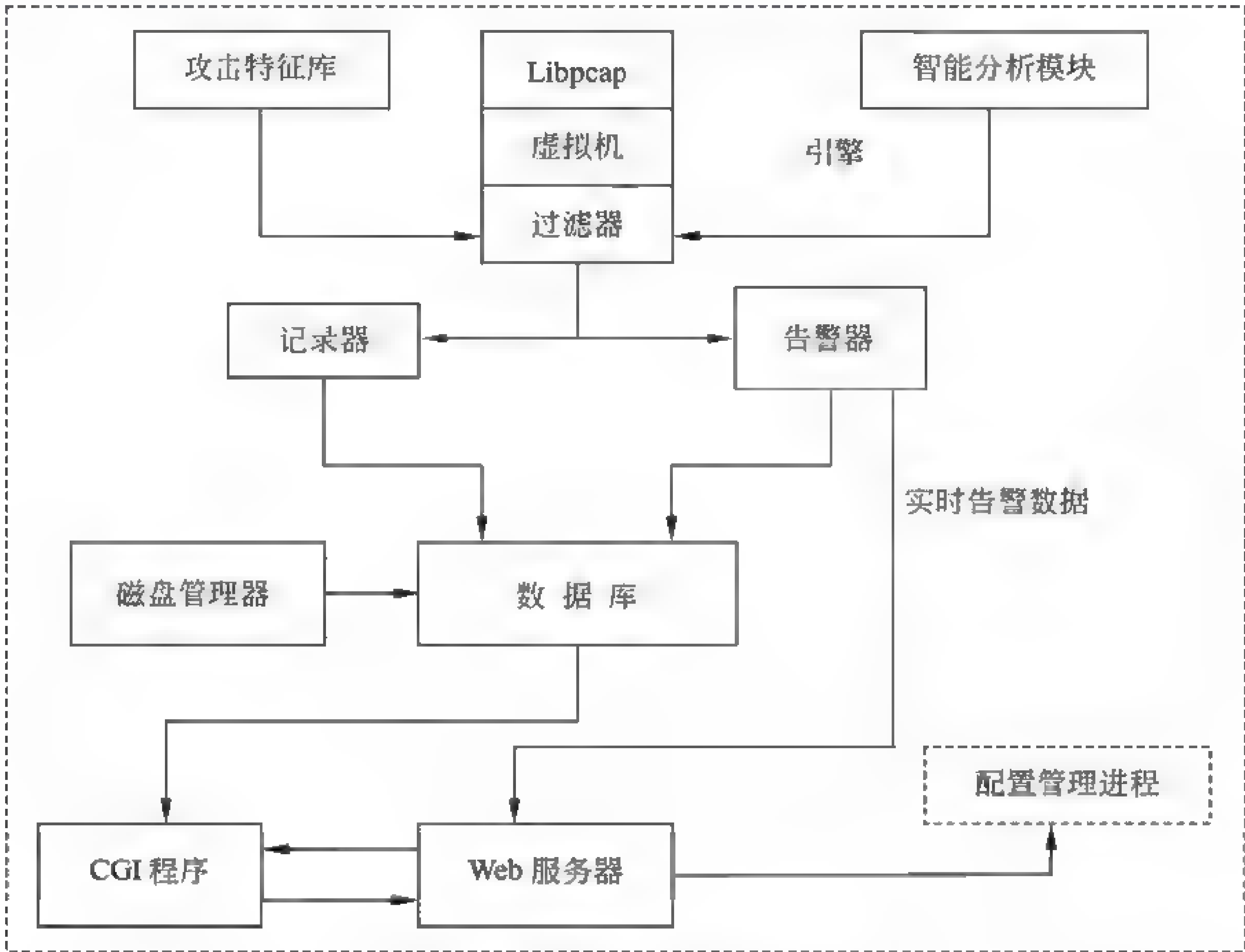


图 4-82　网络检测引擎结构图

检测引擎具有在线升级功能，升级包括攻击特征库的更新和软件程序的更新。

检测引擎的接入对被保护网络是透明的，它对被保护网络的任何流量和请求均不做反应，不影响被保护网络的性能。

2）管理控制台

管理控制台是对检测引擎进行配置、管理和数据查询的软件程序，它可以安装在内网的管理员主机（Windows 2000/NT 操作系统）上。

此外，为了加强对引擎进行访问的用户的管理，RIDS-100 系统设计了一套完善的用户管理机制，每个管理用户配有一把电子钥匙，内装有该用户的密钥和加密算法。用户在对系统进行管理时必须插入自己的钥匙并输入正确的口令。系统构成如表 4-8 所示。

表 4-8 RIDS-100 构成

部件名称	产品形态	安装方式	在系统中的作用
入侵检测引擎	硬件	即插即用	监听被保护网络，检测攻击，实时报警，存储检测到的信息
管理控制台	软件	安装在管理员主机（Windows 2000/NT）	对引擎进行管理、配置，查询数据
电子钥匙	硬件	即插即用	实现用户一次性口令认证

典型应用方案

1）监听、检测发生在内网之间的连接和攻击

如图 4-83 所示，入侵检测引擎与内部网络主机并联，它以隐身模式通过监听口从网络线路上获取数据，然后调用相应的处理模块进行分析处理，如果发现异常事件，则调用告警器，由其根据预定义的处理规则决定调用相应的响应模块。入侵检测引擎还通过管理口与管理主机通信，响应模块可以采取多种手段向系统管理员或被攻击主机报警，也可以主动切断发生攻击的连接。

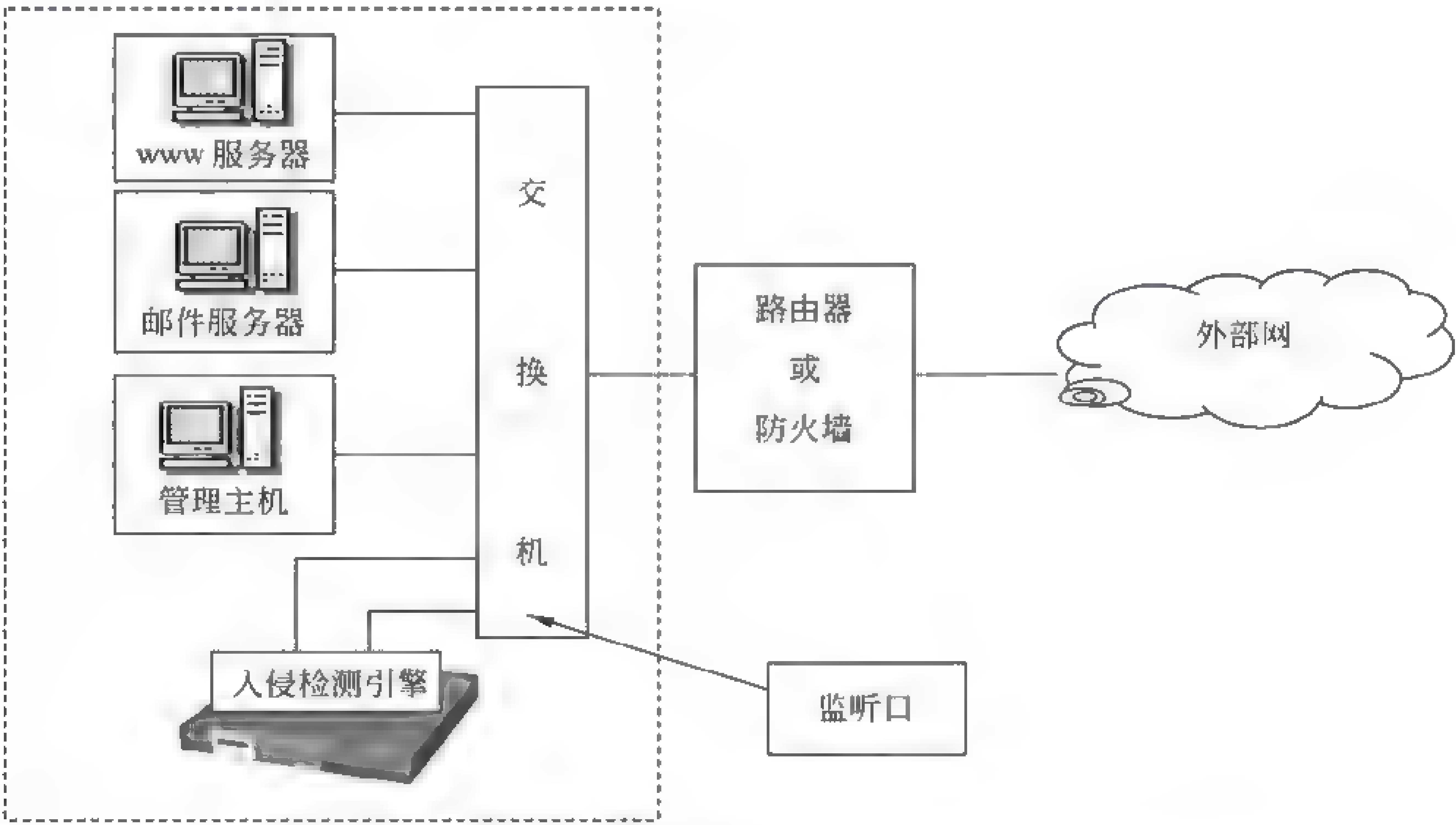


图 4-83 监听、检测内网中发生的所有连接和攻击时引擎的安装方式

2）监听、检测外网对内网的攻击

如图 4-84 所示，防火墙串联在外部网和内网的连接线路上，过滤来自非安全区和 DMZ 区的数据，而入侵检测引擎与防火墙并联，通过监听口监听来自非安全区的数据，并做出相应反应。入侵检测引擎通过管理口与内网的管理主机通信。

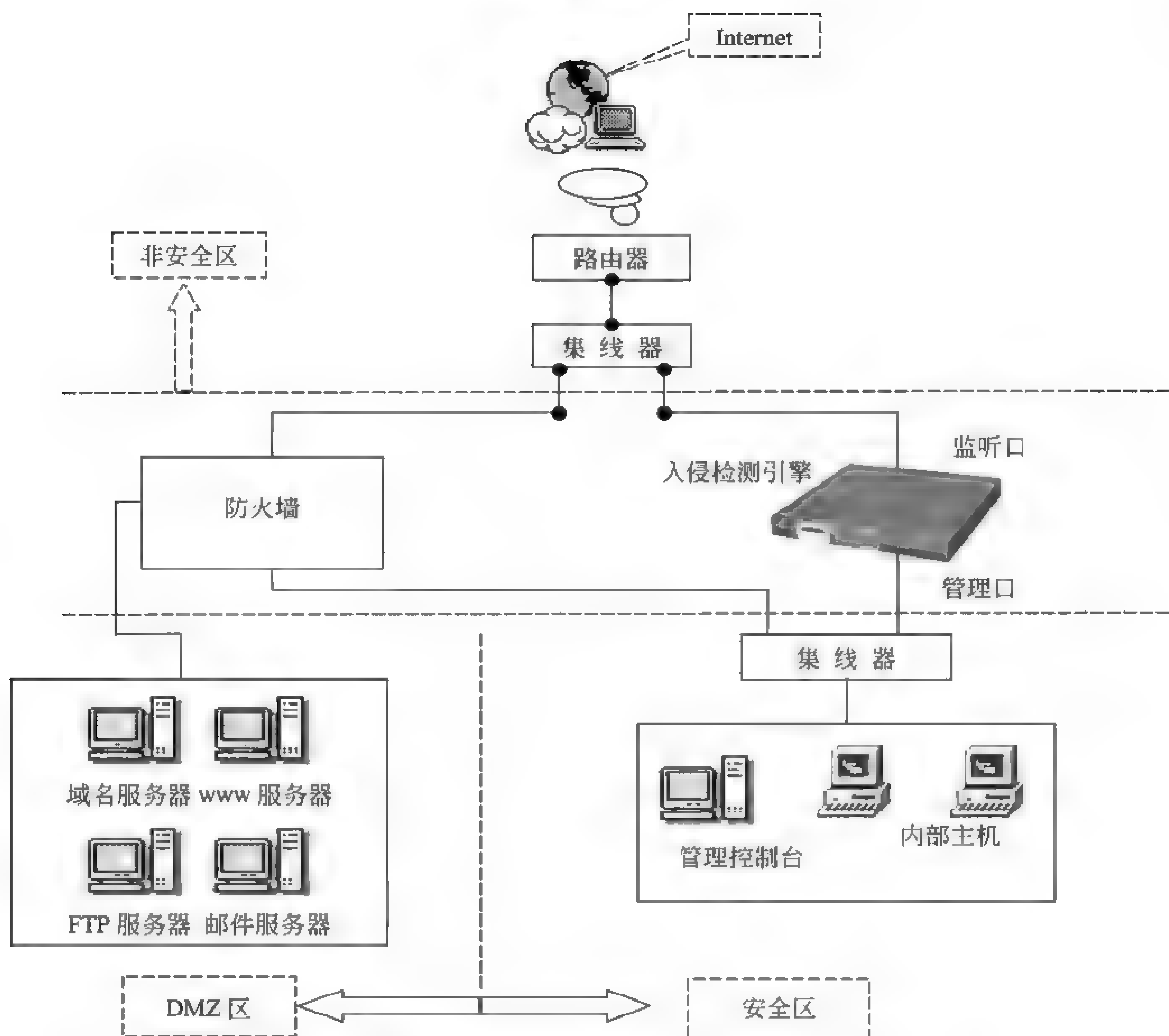


图 4-84　用于监听、检测外网对内网所做的攻击时引擎的安装方式

限于篇幅，只对 RIDS-100 作简要介绍，配置细节在此不作介绍，用户可以自行参看相关的帮助文档和使用手册。

2．Cisco 入侵检测系统 4200

Cisco IDS 4200 系列设备检测器是专用型高性能网络安全“设备”，能够阻止网络上的非法恶意行为，例如黑客发动的攻击。Cisco IDS 检测器能够实时分析流量，使用户能够快速地对安全问题作出反应。

思科著名的思科防御研究小组（C-CRT）将许多高新检测技术结合在一起，包括状态样式识别、协议解析、启发式检测和异常检测，因而能有效消除多种已知和未知的计算机威胁。不仅如此，借助 Cisco 签名微型引擎（SME）技术，还可以更加精细地定制检测器签名，精确调整检测器，检测器错误指示。

检测到非法行为后，检测器可以向管理控制台通报行为细节。另外，Cisco IDS 主动响应系统还能控制路由器、防火墙和交换机等其他系统，为网络提供保护，及时中断非法操作。借助多种多样的管理解决方案，包括 Web 用户界面、命令行界面（CLI）或思科高度可扩展的 CiscoWorkd VPN/安全管理解决方案（VMS），这些设备的安装和管理非常容易。

1）Cisco IDS 解决方案

考虑到企业站点非常复杂，袭击技术多种多样，黑客数量只增不减，必须采用全面的解决方案才能有效预防黑客的袭击。这种解决方案应该能对抗多种袭击技术，并防止在典型袭击过程中执行恶意操作。由于 Cisco IDS 解决方案提供包含 NIDS 和 HIDS 组件的组合解决方案，因而能满足这个要求。NIDS 主要预防网络袭击，HIDS 则主要防止服务器遭受 OS 和应用袭击。

NIDS 检测器安装在多个位置上。最重要的位置是防火墙前面，负责监控进入机构的通信信息。另外，每个重要的网段都安装一个检测器。HIDS 首先部署在面对因特网的服务器上，例如 Web、邮件和 DNS 服务器。由于面向因特网的服务器与后端服务器相连，因此，HIDS 也部署在公司防火墙内的所有其他主要服务器上。

2）Cisco IDS 网络检测器

网络检测器能够为网络设备及服务器上的通信模块提供全面保护。其主要特性如下。

（1）积极响应。系统包含对检测器设备的主动响应功能，用户只需修改 Cisco 路由器上的访问控制表就能让系统自动回避或取消特定连接。回避功能可以临时启用，也可以长久保留。其他网络流量正常流动，只快速、有效地删除来自内部用户或外部入侵者的非法流量。这样，安全操作员就能够快速终止误操作，并防止入侵者访问网络。

（2）全面检测网络袭击。包括检测对路由器和交换机的恶意袭击，检测面向服务器通信模块的第 3 层（或更低层次）袭击，检测探听或映射等企图，例如通常作为实际袭击前兆的呼叫清除和端口清除。

（3）全面检测应用袭击。系统支持多种应用协议，如 HTTP、DNS、文件传输协议（FTP）及其他协议。另外，它还能检测针对易损 CGI 程序发起的多种通信袭击。

（4）以独特的方式预防 DoS。检测 DDoS 代理与黑客之间的通信，预防用于穿越典型 NIDS 技术的分组分片及其他编码技巧技术。

3）Cisco IDS 主机检测器

主机检测器能够为服务器上运行的服务器操作系统和应用提供全面保护。主机检测器安装在每台服务器上，用于保护 OS 和应用。系统利用呼叫截获技术提供纯主动式服务器安全系统。其主要特性如下。

（1）现场预防 OS 和应用袭击。与只有在袭击成功之后才查看记录和反应的基于记录的 HIDS 不同，主机检测器能够在袭击发生之前在呼叫水平上预防袭击。

（2）防止缓冲器溢出袭击。主机检测器能够发现注入代码的执行过程并防止系统受损。两个主要功能如下。

① 保护与用于提供代码的手段无关，即使注入代码未通过线路传输，也能防止袭击。

② 机制使用了即使袭击未知也能防止执行恶意代码的通用签名，对于厂商尚未提供任何补丁程序的未知缓冲器溢出，这种方法能够提供保护。

（3）不断提高完整性。通过控制对二进制、配置数据及其他系统对象的访问，主机检测器能锁定系统。即使是超级用户，也无法篡改系统。通过配置，主机检测器可以不允许修改某些系统设置，以保证设置符合推荐的默认值。这些特性不但能强化服务器操作系统，还能显著提高系统的完整性。

（4）Web 服务器屏蔽。为保护领先的 Web 服务器（IIS、Apache 和 I-Planet），服务器检测器包括特殊屏蔽模块。这些模块基于行为模块，能提供两种主要特性。

① 防止其他程序访问特殊应用资源（甚至在权限用户执行的时候）。

② 防止恶意使用 Web 服务器。借助 Web 服务器专用的行为模式，主机检测器能防止未知袭击，因为识别基于行为模式，且不是每次袭击都需要特殊签名。

（5）防止安全套接层（SSL）加密的 HTTP 袭击。NIDS 不能对用 SSL 加密的 HTTP 请求进行解密。利用这个弱点，黑客可以通过对袭击加密绕过 NIDS。加密后的恶意请求能够悄悄通过 NIDS，然后由 Web 服务器解密并执行，从而成功地利用易损点。另一方面，主机检测器则与 Web 服务器相连，能够在解密后服务前立即截获请求。如果发现请求是恶意的，请求将被丢弃，而不会发送到 Web 服务器，这样就可以预防袭击。

应用

Cisco IDS 4200 系列设备检测器包括三型产品：Cisco IDS 4210、Cisco IDS 4235 和 Cisco IDS 4250。整个 Cisco IDS 设备系列提供多种解决方案，这些解决方案可以集成到多种不同的环境中，包括企业和电信运营商环境。每个设备检测器都能提供多档性能，满足从 45Mbps 到千兆位的带宽要求。

Cisco IDS 4210 可以监控 45Mbps 的流量，适用于 T1/E1 和 T3 环境。

在 200Mbps 速度下，Cisco IDS 4235 可以在交换环境中、多个 T3 子网上以及在 10/100/1000 接口的支持下提供保护。另外，它还可以部署在部分使用的千兆位链路上。

Cisco IDS 4250 不但能以 500Mbps 的速度支持无与伦比的性能，还能保护千兆位子网以及正在穿越交换机（从多个子网汇集流量）的流量。

检测器几乎可以放置在需要安全可视性的企业网的任何网段上。

4.5.3　入侵防御系统

1. 入侵防御系统概述

随着网络攻击技术的发展，对安全技术提出了新的挑战。防火墙技术和 IDS 自身具

有的缺陷阻止了它们进一步的发展。如防火墙不能阻止内部网络的攻击，对于网络上流行的各种病毒也没有很好的防御措施；IDS 只能检测入侵而不能实时地阻止攻击，而且 IDS 具有较高的漏报和误报率。

在这种情况下，入侵防御系统（Intrusion Prevention System，IPS）成了新一代的网络安全技术。IPS 提供主动、实时的防护，其设计旨在对网络流量中的恶意数据包进行检测，对攻击性的流量进行自动拦截，使它们无法造成损失。IPS 如果检测到攻击企图，就会自动地将攻击包丢掉或采取措施阻断攻击源，而不把攻击流量放进内部网络。

1）IPS 与防火墙的区别

从所处的位置来看，很像传统的防火墙技术。但是，传统防火墙只能对网络层和传输层进行检查，不能检测应用层的内容。防火墙的包过滤技术不会针对每一个字节进行检查，因而很多攻击将不会被发现，而 IPS 不仅可以做到对流量进行逐字节的检查，而且可以将经过的数据包还原为完整的数据流，通过对数据流的监控来发现正在进行的网络攻击。

2）IPS 与 IDS 的区别

IPS 和 IDS 的部署方式不同。串接式部署是 IPS 和 IDS 区别的主要特征，IDS 产品在网络中是旁路式工作，IPS 产品在网络中是串接式工作。串接式工作保证所有网络数据都经过 IPS 设备，IPS 检测数据流中的恶意代码，核对策略，在未转发到服务器之前，将信息包或数据流拦截，如图 4-85 所示。由于是在线操作，因而能保证处理方法适当而且可预知。

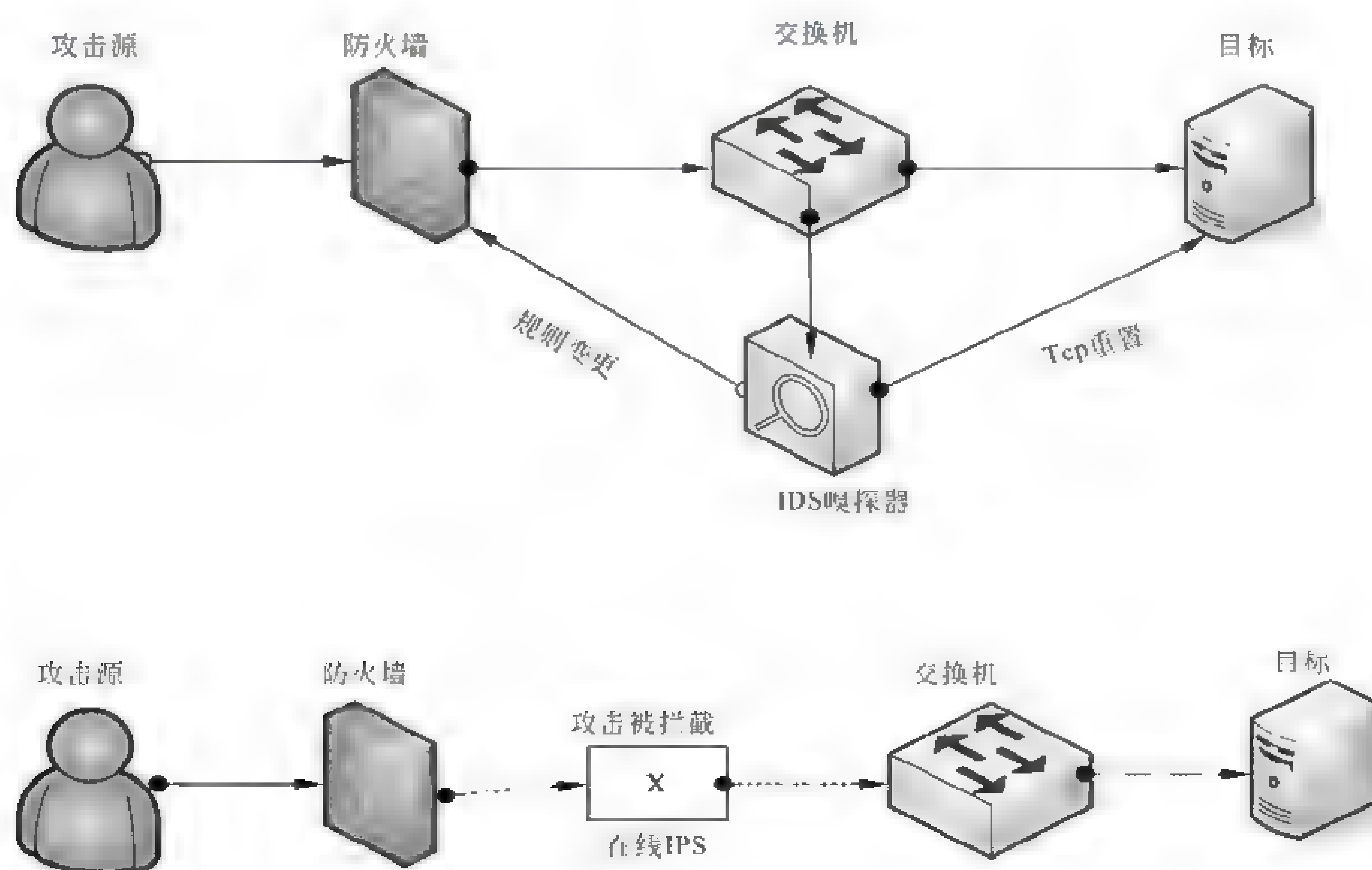


图 4-85 IDS 与 IPS 的区别

IPS 系统根据部署方式可以分为三类：基于主机的入侵防护（HIPS）、基于网络的入侵防护（NIPS）和应用入侵防护（AIP）。

从 IPS 的功能模式来看，必须具备如下技术特征。

（1）嵌入式运行。只有以嵌入模式运行的 IPS 设备才能够实现实时的安全防护，实时阻拦所有可疑的数据包。

（2）深入分析和控制。IPS 必须具有深入分析能力，以确定哪些恶意流量已经被拦截，根据攻击类型、策略等来确定哪些流量应该被拦截。

（3）入侵特征库。高质量的入侵特征库是 IPS 高效运行的必要条件，IPS 还应该定期升级入侵特征库，并快速应用到所有传感器。

（4）高效处理能力。IPS 必须具有高效处理数据包的能力，对整个网络性能的影响保持在低水平。

2．入侵防御系统的原理

IPS 是通过直接嵌入到网络流量中来实现这一功能的，即通过一个端口接收来自外部系统的流量，经过检查确认其中不包含异常活动或可疑内容后，再通过另外一个端口将它传送到内部系统中。这样有问题的数据包，以及所有来自同一数据流的后续数据包，都能在 IPS 设备中被清除掉。如果有攻击者利用 Layer2（数据链路层）至 Layer7（应用层）的漏洞发起攻击，IPS 能够从数据流中检查出这些攻击并加以阻止，传统的防火墙只能对 Layer3（网络层）或 Layer4（传输控制层）进行检查，不能检测应用层的内容。防火墙的包过滤技术不会针对每一个字节进行检查，因而也就无法发现攻击活动，而 IPS 可以做到逐一字节的检查数据包。所有流经 IPS 的数据包都被分类，分类的依据是数据包中的报头信息，如源 IP 地址和目的 IP 地址、端口号和应用域。每种过滤器负责分析相对应的数据包。通过检查的数据包可以继续前进，包含恶意内容的数据包就会被丢弃，被怀疑的数据包则需要接受进一步的检查。IPS 的基本工作原理如图 4-86 所示。

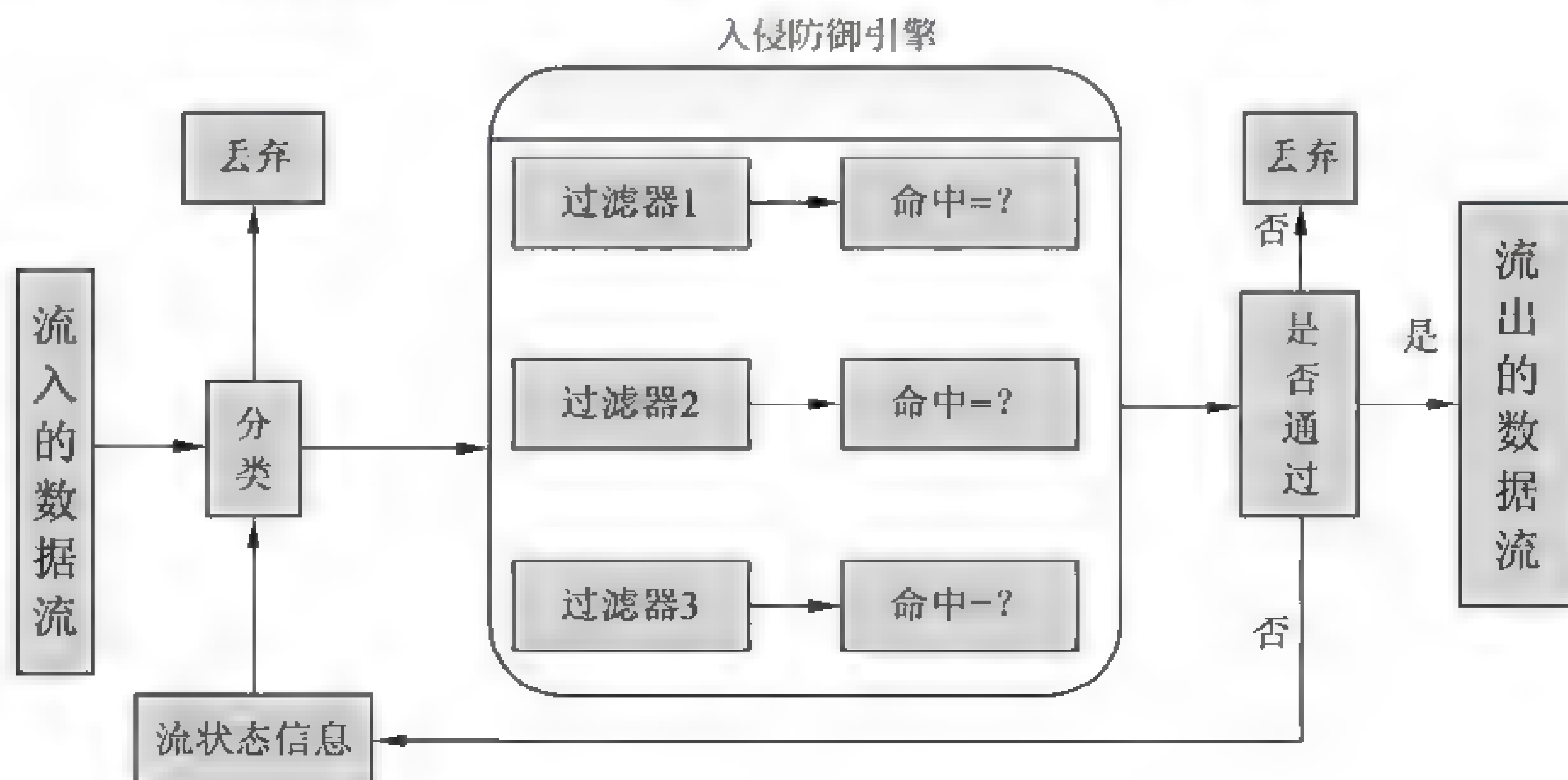


图 4-86　IPS 原理图

（1）根据数据包头和流信息如源目的地址、源目的端口和应用层关键的信息每个数据包都会被分类，同时协议类型和流量统计等信息都送到流处理模块分析、审计。

（2）根据数据报的分类，相关的过滤器将被调用，用于检查数据包的流状态信息。

（3）所有相关过滤器都是并行使用，如果任何数据报符合过滤规则，则数据包中 match 位置 1 的数据报将被丢弃，与之相关的流信息将更新，指示系统删除关于该数据流的信息。

针对不同的攻击行为，IPS 需要不同的过滤器。每种过滤器都设有相应的过滤规则，为了确保准确性，这些规则的定义非常广泛。在对传输内容进行分类时，过滤引擎还需要参照数据包的信息参数，并将其解析至一个有意义的域中进行上下文分析，以提高过滤准确性。过滤器引擎集合了流水和大规模并行处理硬件，能够同时执行数千次的数据包过滤检查。并行过滤处理可以确保数据包能够不间断地快速通过系统，不会对速度造成影响。

如果在网络边界检查到攻击包的同时将其直接抛弃，则攻击包将无法到达目标，从而可以从根本上避免黑客的攻击。这样，在新漏洞出现后，只需要撰写一个过滤规则，就可以防止此类攻击的威胁了。

3．IPS 的检测技术

目前大部分 IPS 的检测技术沿用了传统 IDS 的相关技术，本文在原有检测技术基础上，根据现在网络上流行的各种攻击技术提炼并分析了针对这些攻击的更细粒度的检测技术。为了提高检测的精确度，IPS 最好使用多种综合检测机制，实现深度检测。

（1）基于特征的匹配技术。特征匹配技术的前提是建立入侵特征库。入侵特征库建立的依据是攻击技术的特征、应用协议设计上的缺陷和漏洞、系统误用模式等。当数据包到来时，该技术通过检测数据包内容来提取相关信息，然后和入侵特征库中规则进行匹配，从而发现违背安全策略的行为。一般来讲，一种攻击模式可以用一个过程（如执行一条指令）或一个输出（如获得权限）来表示。该方法的最大优点是只需要收集相关的特征集合，显著减少系统负担，且已相当成熟。它与病毒防火墙采用的方法一样，检测准确率和效率都相当高。但是，该方法存在的弱点是需要不断地升级特征库以对付不断出现的攻击技术，且不能检测到未知的攻击，也不能检测混合型的攻击。

（2）协议分析技术。协议分析是一种较新的入侵检测技术，它充分利用网络协议的高度有序性，并结合高速数据包捕捉和协议分析，来快速检测某种攻击特征。协议分析正在逐渐进入成熟应用阶段。协议分析能够理解不同协议的工作原理，以此分析这些协议的数据包，来寻找可疑或不正常的访问行为。协议分析不仅仅基于协议标准。通过协议分析，IPS 能够针对反 IDS 的插入（insertion）与规避（evasion）攻击进行检测。

与传统防火墙不同的是，IPS 不但要分析和跟踪 IP、ICMP、UDP、TCP 这几种网络层、传输层的协议，而且还要对 HTTP、HTTPS、FTP、TFTP、SNMP、Telnet、SMTP、

POP、DNS、RPC、LDAP、ICQ、MSN 和 Yahoo Messenger 等众多的应用层协议进行分析、跟踪。在该技术中，所有流经 IPS 的数据包首先经过预处理，这个预处理过程主要完成对数据包的重组，以便 IPS 能够看清楚具体的应用协议。在此基础上，IPS 根据不同应用协议的特征与攻击方式，将重组后的包进行筛选，将一些可疑数据包送入专门的特征库进行对比。由于经过了筛选，可疑数据量大大减少，因此可以大幅度减少 IPS 处理的工作量，同时降低误报率。

（3）抗 DDoS/DoS 技术。DDoS 攻击是在 DoS 攻击的基础上产生的一类攻击方式，攻击者使用协同控制的方式控制多台网络主机同时向目标主机发起拒绝服务攻击，构成对因特网的威胁。检测此类攻击可有两种方法：基于数据包特征的分析和基于流量的统计。

（4）智能化检测技术。随着人工智能和数据挖掘技术的发展，出现了智能化检测技术。该方法是现阶段常用的神经网络、遗传算法和模糊技术等，这些方法用于入侵特征的辨识与泛化。利用具有学习能力的专家系统，可以实现知识库的不断升级与扩展，使系统的防范能力不断增强，具有更广泛的应用前景。此外，由于信息和数据量庞大，借用数据挖掘的方法，包括关联、序列等，可以有效提高入侵检测的精确性。

（5）蜜罐技术。美国 L.Spizner 一个著名的蜜罐技术专家，他曾对蜜罐做了这样的定义：蜜罐是一种资源，它的价值是被攻击或攻陷。这就意味着蜜罐是用来被探测、被攻击甚至最后被攻陷的，蜜罐不会修补任何东西，这样就为使用者提供了额外的、有价值的信息。一个合格的蜜罐需要具有如下功能：发现攻击、产生警告、强大的记录能力、欺骗和协助调查。

为了吸引攻击者，通常在蜜罐系统上留下一些安全后门，或者放置一些网络攻击者希望得到的敏感信息，当然这些都是虚假的信息。当有攻击者进入时，蜜罐将把攻击者从关键系统引开，同时开始收集攻击者的活动信息，并且吸引攻击者在系统停留，便于记录攻击者的行为。蜜罐技术最重要的功能也就是对攻击者所有操作和行为进行监视和记录，然后把结果保存在日志服务器上，便于管理员查看与分析，为进一步完善系统的安全措施提供依据。

蜜罐不会直接提高计算机网络安全，但它却是一种不可缺少的主动防御技术，目前很多 IPS 产品中都集成蜜罐技术。

4．IPS 存在的问题

目前 IPS 技术面临着很多挑战，主要有以下 4 方面。

（1）单点故障。设计要求 IPS 必须以嵌入模式工作在网络中，这就可能造成单点故障。如果嵌入式 IPS 设备出现问题，就会严重影响网络的正常运转；如果 IPS 因故障而关闭，则合法用户无法访问网络提供的服务。

（2）性能瓶颈。IPS 嵌入式接入，即使 IPS 设备不出现故障，仍然是一个潜在的网络瓶颈。所有流量的数据包都通过 IPS 进行检测，当检测特征库规则数量庞大时，不可

避免地给传输带来延迟。

（3）误报率和漏报率。在繁忙的网络当中，一旦生成了警报，最基本的要求就是 IPS 能够对警报进行有效处理。如果入侵特征编写得不是十分完善，那么“误报”就有了可乘之机，导致合法流量也有可能被意外拦截。对于实时在线的 IPS 来说，一旦拦截了“攻击性”数据包，就会对来自可疑攻击者的所有数据流进行拦截。如果产生了误报警报的流量恰好是某个合法用户，其结果可想而知，这个用户整个会话就会被关闭，而且此后该用户所有重新连接到网络的合法访问都会被“尽职尽责”的 IPS 拦截。

（4）规则库更新。IPS 规则库与病毒库一样，需要不断更新。但是安全事件的种类和数量太多，不易提取特征，IPS 更新规则库难度较大。

4.6 访问控制技术

4.6.1 访问控制技术概述

互联网络的蓬勃发展，为信息资源的共享提供了更加完善的手段，企业在信息资源共享的同时也要阻止非授权用户对企业敏感信息的访问。访问控制的目的是为了保护企业在信息系统中存储和处理的信息的安全。

1. 访问控制的基本模型

访问控制是指主体依据某些控制策略或权限对客体本身或是其资源进行的不同授权访问。访问控制包括三个要素：主体、客体和控制策略。访问控制模型是一种从访问控制的角度出发，描述安全系统，建立安全模型的方法。

（1）主体（Subject，S）：是可以对其他实体施加动作的主动实体。有时也称其为用户（User，U）或访问者（被授权使用计算机的人员）。主体的含义是广泛的，可以是用户所在的组织（称为用户组）、用户本身，也可以是用户使用的计算机终端、卡机和手持终端（无线）等，甚至可以是应用服务程序或进程。

（2）客体（Object，O）：是接受其他实体访问的被动实体。客体的概念也很广泛，凡是可以被操作的信息、资源、对象都可以认为是客体。在信息社会中，客体可以是信息、文件和记录等的集合体，也可以是网路上的硬件设施，无线通信中的终端，甚至一个客体可以包含另外一个客体。

（3）控制策略（KS）：是主体对客体的操作行为集和约束条件集。简单地讲，控制策略是主体对客体的访问规则集，这个规则集直接定义了主体对客体的作用行为和客体对主体的条件约束。访问策略体现了一种授权行为，也就是客体对主体的权限允许，这种允许不超越规则集，由其给出。

当主体 S 提出一系列正常的请求信息 I1，…，In，通过信息系统的入口到达控制规则集 KS 监视的监控器，由 KS 判断是否允许或拒绝这次请求，因此这种情况下，必须

先要确认是合法的主体，而不是假冒的欺骗者，也就是对主体进行认证。主体通过验证，才能访问客体，但并不保证其有权限可以对客体进行操作。客体对主体的具体约束由访问控制表来控制实现，对主体的验证一般会鉴别用户的标识和用户密码。用户标识（User Identification，UID）是一个用来鉴别用户身份的字符串，每个用户有且只能有唯一的一个用户标识，以便与其他用户区别。当一个用户注册进入系统时，他必须提供其用户标识，然后系统执行一个可靠的审查来确信当前用户是对应用户标识的那个用户。

访问控制的实现首先要考虑对合法用户进行验证，然后是对控制策略的选用与管理，最后要对没有非法用户或是越权操作进行管理。所以，访问控制包括认证、控制策略实现和审计三方面的内容。

（1）认证。主体对客体的识别认证和客体对主体检验认证。主体和客体的认证关系是相互的，当一个主体受到另外一个客体的访问时，这个主体也就变成了客体。一个实体可以在某一时刻是主体，而在另一时刻是客体，这取决于当前实体的功能是动作的执行者还是动作的被执行者。

（2）控制策略的具体实现。如何设定规则集合从而确保正常用户对信息资源的合法使用，既要防止非法用户，也要考虑敏感资源的泄漏。对于合法用户而言，更不能越权行使控制策略所赋予其权利以外的功能。

（3）审计。审计的重要意义在于，例如客体的管理者即管理员有操作赋予权，他有可能滥用这一权利，这是无法在策略中加以约束的。必须对这些行为进行记录，从而达到威慑和保证访问控制正常实现的目的。

2．访问控制的实现技术

建立访问控制模型和实现访问控制都是抽象和复杂的行为，实现访问的控制不仅要保证授权用户使用的权限与其所拥有的权限对应，制止非授权用户的非授权行为，还要保证敏感信息的交叉感染。为了便于讨论这一问题，我们以文件的访问控制为例对访问控制的实现做具体说明。通常用户访问信息资源（文件或是数据库），可能的行为有读、写和管理。为方便起见，用 Read 或是 R 表示读操作，Write 或是 W 表示写操作，Own 或是 O 表示管理操作。之所以将管理操作从读写中分离出来，是因为管理员也许会对控制规则本身或是文件的属性等做修改。

1）访问控制矩阵

访问控制矩阵（Access Control Matrix，ACM）是通过矩阵形式表示访问控制规则和授权用户权限的方法。也就是说，对每个主体而言，都拥有对哪些客体的哪些访问权限；而对客体而言，又有哪些主体对他可以实施访问。将这种关连关系加以阐述，就形成了控制矩阵。其中，特权用户或特权用户组可以修改主体的访问控制权限。访问控制的实现如表 4-9 所示。

表 4-9　访问控制矩阵

	Object 1	Object 2	…	Object *j*	…
Subject 1	Read，write	Own，read，write	…	read	…
Subject 2	read	Read，write	…	Own，read，write	…
…	…	…	…	…	…
Subject *i*	Own，read，write	read	…	Read，write	…
…	…	…	…	…	…

访问矩阵是以主体为行索引，以客体为列索引的矩阵，矩阵中的每一个元素表示一组访问方式，是若干访问方式的集合。矩阵中第 i 行第 j 列的元素记录着第 i 个主体 S_i 可以执行的对第 j 个客体 O_j 的访问方式，如 M_{ij} 等于表示 S_i 可以对 O_j 进行读和写访问。

访问控制矩阵的实现很易于理解，但是查找和实现起来有一定的难度。而且，如果用户和文件系统要管理的文件很多，那么控制矩阵将会成几何级数增长。因为在大型系统中访问矩阵很大而且其中会有很多空值，所以目前使用的实现技术都不是保存整个访问矩阵，而是基于访问矩阵的行或者列来保存信息，下面分别介绍。

2）访问控制表

访问控制表（Access Control Lists，ACLs）是目前最流行、使用最多的访问控制实现技术。每个客体有一个访问控制表，是系统中每一个有权访问这个客体的主体的信息。这种实现技术实际上是按列保存访问矩阵。访问控制表提供了针对客体的方便的查询方法，通过查询一个客体的访问控制表很容易决定某一个主体对该客体的当前访问权限。删除客体的访问权限也很方便，把该客体的访问控制表整个替换为空表即可。但是用访问控制表来查询一个主体对所有客体的所有访问权限是很困难的，必须查询系统中所有客体的访问控制表来获得其中每一个与该主体有关的信息。类似地，删除一个主体对所有客体的所有访问权限也必须查询所有客体的访问控制表，删除与该主体相关的信息。一些流行的操作系统使用了简化的访问控制表来实现它们简单的访问控制安全机制，例如 UNIX 的保护位机制就是这样一种简化形式的访问控制表。在这些系统中，访问控制表只包括客体主人、主人所属主体组等对该客体的访问权限，所以访问控制表可以很小。另一方面，一些系统采用了许多大型的访问控制表来实现其访问控制，其中包含了一些很复杂的规则来决定系统中主体何时以及以何种方式对客体进行访问。

3）能力表

能力表（Capabilities Lists）对应于访问控制表，这种实现技术实际上是按行保存访问矩阵。每个主体有一个能力表，是该主体对系统中每一个客体的访问权限信息。使用能力表实现的访问控制系统可以很方便地查询某一个主体的所有访问权限，只需要遍历这个主体的能力表即可。然而，查询对某一个客体具有访问权限的主体信息就很困难了，必须查询系统中所有主体的能力表。20 世纪 70 年代，很多操作系统的访问控制安全机

制是基于能力表实现的，但并没有取得商业上的成功，现代的操作系统大多改用基于访问控制表的实现技术，只有少数实验性的安全操作系统使用基于能力表的实现技术。在一些分布式系统中，也使用了能力表和访问控制表相结合的方法来实现其访问控制安全机制。

4）授权关系表

访问矩阵也有既不对应于行也不对应于列的实现技术，那就是对应访问矩阵中每一个非空元素的实现技术——授权关系表(authorization relations)。授权关系表的每一行(或者说元组）就是访问矩阵中的一个非空元素，是某一个主体对应于某一个客体的访问权限信息。如果授权关系表按主体排序，查询时就可以得到能力表的效率；如果按客体排序，查询时就可以得到访问控制表的效率。安全数据库系统通常用授权关系表来实现其访问控制安全机制。

3．访问控制表介绍

访问控制表是目前最流行、使用最多的访问控制实现技术。访问控制列表是路由器接口的指令列表，用来控制端口进出的数据包。ACL 适用于所有的被路由协议，如 IP、IPX 和 AppleTalk 等。

ACL 的定义也是基于每一种协议的。如果路由器接口配置成为支持三种协议（IP、AppleTalk 以及 IPX）的情况，那么，用户必须定义三种 ACL 来分别控制这三种协议的数据包。

1）ACL 的作用

（1）可以限制网络流量、提高网络性能。例如，可以根据数据包的协议，指定数据包的优先级。

（2）提供对通信流量的控制手段。例如，可以限定或简化路由更新信息的长度，从而限制通过路由器某一网段的通信流量。

（3）是提供网络安全访问的基本手段。例如，允许主机 A 访问某资源网络，而拒绝主机 B 访问。

（4）可以在路由器端口处决定哪种类型的通信流量被转发或被阻塞。例如，用户可以允许 E-mail 通信流量被路由，拒绝所有的 Telnet 通信流量。

2）ACL 的执行过程

一个端口执行哪条 ACL，这需要按照列表中的条件语句执行顺序来判断。如果一个数据包的报头跟表中某个条件判断语句相匹配，那么后面的语句就将被忽略，不再进行检查。数据包只有在跟第一个判断条件不匹配时，它才被交给 ACL 中的下一个条件判断语句进行比较。如果匹配（假设为允许发送），则不管是第一条还是最后一条语句，数据都会立即发送到目的接口。如果所有的 ACL 判断语句都检测完毕，仍没有匹配的语句出口，则该数据包将视为被拒绝而被丢弃（这里要注意，ACL 不能对本路由器产生的数据包进行控制）。

3）ACL 的分类

目前有两种主要的 ACL：标准 ACL 和扩展 ACL。这两种 ACL 的区别是，标准 ACL 只检查数据包的源地址；扩展 ACL 既检查数据包的源地址，也检查数据包的目的地址，同时还可以检查数据包的特定协议类型、端口号等。网络管理员可以使用标准 ACL 阻止来自某一网络的所有通信流量，或者允许来自某一特定网络的所有通信流量，或者拒绝某一协议簇（如 IP）的所有通信流量。扩展 ACL 比标准 ACL 提供了更广泛的控制范围。例如，网络管理员如果希望做到"允许外来的 Web 通信流量通过，拒绝外来的 FTP 和 Telnet 等通信流量"，那么，他可以使用扩展 ACL 来达到目的，标准 ACL 不能控制得这么精确。

4）ACL 的配置

ACL 的配置分为如下两步。

（1）在全局配置模式下，使用下列命令创建 ACL：

```
Router(config)# access-list access-list-number {permit | deny }
{test-conditions}
```

其中，access-list-number 为 ACL 的表号。人们使用较频繁的表号是标准的 IP ACL（1～99）和扩展的 IP ACL（100～199）。在路由器中，如果使用 ACL 的表号进行配置，则列表不能插入或删除行。如果列表要插入或删除一行，必须先去掉所有 ACL，然后重新配置。当 ACL 中条数很多时，这种改变非常烦琐。一个比较有效的解决办法是：在远程主机上启用一个 TFTP 服务器，先把路由器配置文件下载到本地，利用文本编辑器修改 ACL 表，然后将修改好的配置文件通过 TFTP 传回路由器。这里需要特别注意的是，在 ACL 的配置中，如果删掉一条表项，其结果是删掉全部 ACL，所以在配置时一定要小心。

（2）在接口配置模式下，使用 access-group 命令 ACL 应用到某一接口上：

```
Router(config-if)# {protocol} access-group access-list-number {in | out }
```

其中，in 和 out 参数可以控制接口中不同方向的数据包，如果不配置该参数，默认为 out。ACL 在一个接口可以进行双向控制，即配置两条命令，一条为 in，一条为 out，两条命令执行的 ACL 表号可以相同，也可以不同。但是，在一个接口的一个方向上，只能有一个 ACL 控制。

5）标准 ACL 举例

使用标准版本的 access-list 全局配置命令来定义一个带有数字的标准 ACL。

例如：

```
access-list 1 permit 172.16.0.0  0.0.255.255
```

使用这个命令的 no 形式，可以删除一个标准 ACL。语法是：

```
Router(config)# no access-list access-list-number
```

例如：

```
no access-list 1
```

命令 ip access-group 将一个存在的扩展 ACL 和一个端口关联。记住：一个端口的一个方向的某套协议，只允许存在一个 ACL。

下面以图 4-87 的结构为例，介绍标准 ACL 的使用。

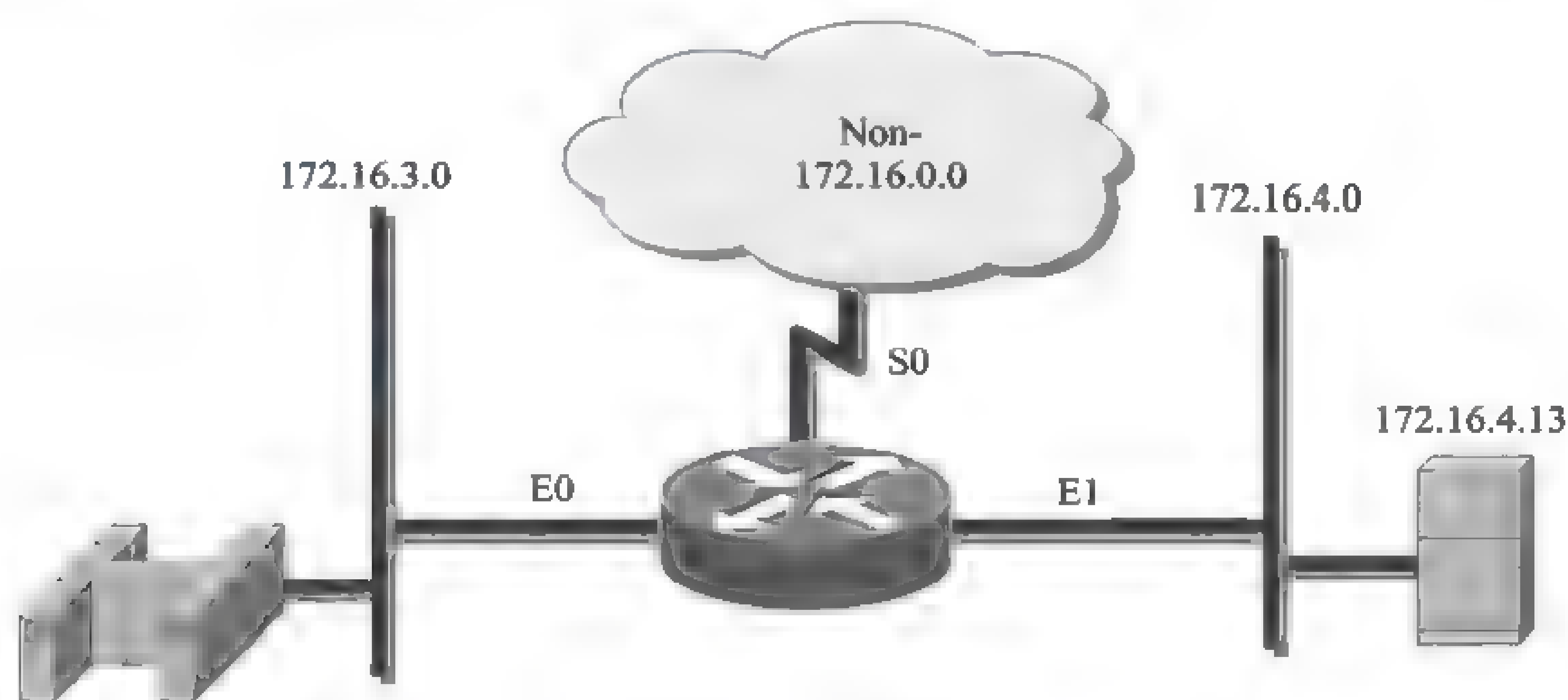


图 4-87　示例结构图

实例：E0 和 E1 端口只允许来自于网络 172.16.0.0 的数据报被转发，其余的将被阻止。

第一个 ACL 命令用 permit 允许来自于此指定网络的数据流，通配掩码 0.0.255.255 表明要检查匹配 IP 地址中的网络位（前 16 位）。最后将 ACL 关联到端口 E0 和 E1。

```
access-list 1 permit 172.16.0.0  0.0.255.255
(implicit deny all - not visible in the list)
(access-group 1 deny 0.0.0.0-255.255.255.255)
interface ethernet 0
ip access-group 1 out
interface ethernet 1
ip access-group 1 out
```

4．访问控制的模型发展

访问控制安全模型一般包括主体、客体，以及为识别和验证这些实体的子系统和控制实体间访问的参考监视器。由于网络传输的需要，访问控制的研究方发展很快，有许多访问控制模型被提出来。建立规范的访问控制模型，是实现严格访问控制策略所必须

的。20世纪70年代，Harrison、Ruzzo和Ullman提出了HRU模型。接着，Jones等人在1976年提出了Take-Grant模型。随后，1985年美国军方提出可信计算机系统评估准则TCSEC，其中描述了两种著名的访问控制策略：自主访问控制模型（DAC）和强制访问控制模型（MAC）。基于角色的访问控制（RBAC）是由Ferraiolo和Kuhn在1992年提出的。考虑到网络安全和传输流，又提出了基于对象和基于任务的访问控制。后面几节将对一些重要模型作简要阐述。

4.6.2 传统访问控制技术

1．自主型访问控制

允许合法用户以用户或用户组的身份访问策略规定的客体，同时阻止非授权用户访问客体，某些用户还可以自主地把自己所拥有的客体的访问权限授予其他用户。自主访问控制又称为任意访问控制。Linux、UNIX、Windows NT或是Server版本的操作系统都提供自主访问控制的功能。在实现上，首先要对用户的身份进行鉴别，然后就可以按照访问控制列表所赋予用户的权限允许和限制用户使用客体的资源。主体控制权限的修改通常由特权用户或是特权用户（管理员）组实现。

自主访问控制模型的特点是授权的实施主体（可以授权的主体；管理授权的客体；授权组）自主负责赋予和回收其他主体对客体资源的访问权限。DAC模型一般采用访问控制矩阵和访问控制列表来存放不同主体的访问控制信息，从而达到对主体访问权限的限制目的。

自主访问控制对用户提供的这种灵活的数据访问方式，使得DAC广泛应用在商业和工业环境中。但是DAC技术存在明显的不足，主要体现在以下几方面。

（1）既然主体可任意在系统中规定谁可以访问它们的资源，那么系统管理就难以确定哪些用户对哪些资源有访问权限，不利于实现统一的全局访问控制。

（2）在许多组织中，用户对他们所能访问的资源并不具有所有权，组织本身才是系统中资源的真正拥有者。而且，各组织希望访问控制实现能与组织内部的安全策略相一致，并由管理部门统一实施访问控制，不允许用户自主地处理，而DAC却存在着用户滥用职权的问题。

（3）用户间的关系不能在系统中体现出来，不易管理。

（4）信息容易泄露，不能抵御特洛伊木马的攻击。特洛伊木马是嵌入在合法程序中的一段以窃取或破坏信息为目的的恶意代码。在自主型访问控制下，一旦带有特洛伊木马的应用程序被激活，特洛伊木马便可以任意泄露和破坏接触到的信息，甚至改变这些信息的访问授权模式。

2．强制型访问控制

最开始为了实现比DAC更为严格的访问控制策略，美国政府和军方开发了各种各样的控制模型，这些方案或模型都有比较完善的和详尽的定义。随后，逐渐形成强制访

问控制模型（Mandatory Access Control Model，MAC Model），并得到广泛的商业关注和应用。在 DAC 访问控制中，用户和客体资源都被赋予一定的安全级别，用户不能改变自身和客体的安全级别，只有管理员才能够确定用户和组的访问权限。和 DAC 模型不同的是，MAC 是一种多级访问控制策略，它的主要特点是系统对访问主体和受控对象实行强制访问控制，系统事先给访问主体和受控对象分配不同的安全级别属性，在实施访问控制时，系统先对访问主体和受控对象的安全级别属性进行比较，再决定访问主体能否访问该受控对象。MAC 对访问主体和受控对象标识两个安全标记：一个是具有偏序关系的安全等级标记；另一个是非等级分类标记。安全等级的层次在上节做过阐述，主体和客体在分属不同的安全类别时，都属于一个固定的安全类别 SC，SC 就构成一个偏序关系（如 TS 表示绝密级，就比密级 S 要高）。当主体 s 的安全类别为 TS，而客体 o 的安全类别为 S 时，用偏序关系可以表述为 $SC(s) \geq SC(o)$。考虑到偏序关系，主体对客体的访问主要有如下 4 种方式。

（1）向下读（rd，read down）：主体安全级别高于客体信息资源的安全级别时允许查阅的读操作。

（2）向上读（ru，read up）：主体安全级别低于客体信息资源的安全级别时允许的读操作。

（3）向下写（wd，write down）：主体安全级别高于客体信息资源的安全级别时允许执行的动作或是写操作。

（4）向上写（wu，write up）：主体安全级别低于客体信息资源的安全级别时允许执行的动作或是写操作。

由于 MAC 通过分级的安全标签实现了信息的单向流通，因此它一直被军方采用，其中最著名的是 Bell-LaPadula 模型和 Biba 模型。Bell- LaPadula 模型具有只允许向下读、向上写的特点，可以有效地防止机密信息向下级泄露；Biba 模型则具有不允许向下读、向上写的特点，可以有效地保护数据的完整性。

MAC 的不足主要体现在以下两方面。

（1）用户共享数据的机制不灵活。MAC 不允许一个进程生成共享文件，防止进程通过共享文件将信息从一个进程转移到另一个进程，但这对合法用户却是一种限制。

（2）应用的领域比较窄，使用不灵活，一般只用于军方等具有明显等级观的行业领域。

尽管很多学者对 MAC 进行了种种改进，使得 MAC 技术更加完善，但从总体上看，这些改进大都针对具体应用开发，灵活性差，所产生的影响不大。

MAC 模型和 DAC 模型属于传统的访问控制模型，对这两种模型研究的也比较充分。在实现上，MAC 和 DAC 通常为每个用户赋予对客体的访问权限规则集，考虑到管理的方便，在这一过程中还经常将具有相同职能的用户聚为组，然后再为每个组分配许可权。用户自主地把自己所拥有的客体的访问权限授予其他用户的这种做法，其优点是显而易

见的。但是如果企业的组织结构或是系统的安全需求出于变化的过程中时，那么就需要进行大量繁琐的授权变动，系统管理员的工作将变得非常繁重，更主要的是容易发生错误造成一些意想不到的安全漏洞。考虑到上述因素，我们引入新的机制加以解决。首先要介绍一下角色的概念，角色（role）是指一个可以完成一定事务的命名组，不同的角色通过不同的事务来执行各自的功能。事务（transaction）是指一个完成一定功能的过程，可以是一个程序或程序的一部分。角色是代表具有某种能力的人或是某些属性的人的一类抽象。角色和组的主要区别在于：用户属于组是相对固定的，而用户能被指派到哪些角色则受时间、地点、事件等诸多因素影响。角色比组的抽象级别要高。角色和组的关系可以这样考虑，作为饰演的角色，我是一名学生，我就只能享有学生的权限（区别于老师），但是我又处于某个班级中，就同时只能享有本组组员的权限。

4.6.3　基于角色的访问控制技术

基于角色的访问控制（Role-based Access，RBAC）模型的基本思想是将访问许可权分配给一定的角色，用户通过饰演不同的角色获得角色所拥有的访问许可权。这是因为在很多实际应用中，用户并不是可以访问的客体信息资源的所有者（这些信息属于企业或公司），这样，访问控制应该基于员工的职务而不是基于员工在哪个组或是谁信息的所有者，即访问控制是由各个用户在部门中所担任的角色来确定的。例如，一个学校可以有教工、老师、学生和其他管理人员等角色。

RBAC 从控制主体的角度出发，根据管理中相对稳定的职权和责任来划分角色，将访问权限与角色相联系，这点与传统的 MAC 和 DAC 将权限直接授予用户的方式不同。通过给用户分配合适的角色，让用户与访问权限相联系。角色成为访问控制中访问主体和受控对象之间的一座桥梁。

角色可以看作是一组操作的集合，不同的角色具有不同的操作集，这些操作集由系统管理员分配给角色。在下面的实例中，假设 Tch1，Tch2，Tch3，…，Tchi 是对应的教师，Stud1，Stud 2，Stud3，…，Studj 是相应的学生，Mng1，Mng 2，Mng 3，…，Mngk 是教务处管理人员，那么老师的权限为 TchMN={查询成绩、上传所教课程的成绩}；学生的权限为 Stud MN={查询成绩、反映意见}；教务管理人员的权限为 MngMN={查询、修改成绩、打印成绩清单}。那么，依据角色的不同，每个主体只能执行自己所制定的访问功能。用户在一定的部门中具有一定的角色，其所执行的操作与其所扮演的角色的职能相匹配，这正是基于角色的访问控制的根本特征，即依据 RBAC 策略，系统定义了各种角色，每种角色可以完成一定的职能，不同的用户根据其职能和责任被赋予相应的角色，一旦某个用户成为某角色的成员，则此用户可以完成该角色所具有的职能。

系统管理员负责授予用户各种角色的成员资格或撤消某用户具有的某个角色。例如，学校新进一名教师 Tchx，那么系统管理员只需将 Tchx 添加到教师这一角色的成员中即可，而无需对访问控制列表做改动。同一个用户可以是多个角色的成员，即同一个

用户可以扮演多种角色，如一个用户可以是老师，同时也可以作为进修的学生。同样，一个角色可以拥有多个用户成员，这与现实是一致的，一个人可以在同一部门中担任多种职务，而且担任相同职务的可能不止一人。因此，RBAC 提供了一种描述用户和权限之间的多对多关系，角色可以划分成不同的等级，通过角色等级关系来反映一个组织的职权和责任关系，这种关系具有反身性、传递性和非对称性特点，通过继承行为形成了一个偏序关系，如 MngMN>TchMN>Stud MN。RBAC 中通常定义不同的约束规则来对模型中的各种关系进行限制，最基本的约束是“相互排斥”约束和“基本限制”约束，分别规定了模型中的互斥角色和一个角色可被分配的最大用户数。RBAC 中引进了角色的概念，用角色表示访问主体具有的职权和责任，灵活地表达和实现了企业的安全策略，使系统权限管理在企业的组织视图这个较高的抽象集上进行，从而简化了权限设置的管理。从这个角度看，RBAC 很好地解决了企业管理信息系统中用户数量多、变动频繁的问题。

相比较而言，RBAC 是实施面向企业的安全策略的一种有效的访问控制方式，其具有灵活性、方便性和安全性的特点，目前在大型数据库系统的权限管理中得到普遍应用。角色由系统管理员定义，角色成员的增减也只能由系统管理员来执行，即只有系统管理员有权定义和分配角色。用户与客体无直接联系，他只有通过角色才享有该角色所对应的权限，从而访问相应的客体。因此，用户不能自主地将访问权限授给别的用户，这是 RBAC 与 DAC 的根本区别所在。RBAC 与 MAC 的区别在于：MAC 是基于多级安全需求的，而 RBAC 则不是。

4.6.4 基于任务的访问控制模型

上述几个访问控制模型都是从系统的角度出发去保护资源（控制环境是静态的），在进行权限的控制时没有考虑执行的上下文环境。数据库、网络和分布式计算的发展，组织任务进一步自动化，与服务相关的信息进一步计算机化，这促使人们将安全问题方面的注意力从独立的计算机系统中静态的主体和客体保护，转移到随着任务的执行而进行动态授权的保护上。此外，上述访问控制模型不能记录主体对客体权限的使用，权限没有时间限制，只要主体拥有对客体的访问权限，主体就可以无数次地执行该权限。考虑到上述原因，我们引入工作流的概念加以阐述。工作流是为完成某一目标而由多个相关的任务（活动）构成的业务流程。工作流所关注的问题是处理过程的自动化，对人和其他资源进行协调管理，从而完成某项工作。当数据在工作流中流动时，执行操作的用户在改变，用户的权限也在改变，这与数据处理的上下文环境相关。传统的 DAC 和 MAC 访问控制技术则无法予以实现，我们讲过的 RBAC 模型，也需要频繁地更换角色，且不适合工作流程的运转。这就迫使我们必须考虑新的模型机制，也就是基于任务的访问控制模型。

基于任务的访问控制模型（Task-based Access Control Model，TBAC Model）是从应用和企业层角度来解决安全问题，以面向任务的观点，从任务（活动）的角度来建立安全模型和实现安全机制，在任务处理的过程中提供动态实时的安全管理。

在 TBAC 中，对象的访问权限控制并不是静止不变的，而是随着执行任务的上下文环境发生变化。TBAC 首要考虑的是在工作流的环境中对信息的保护问题：在工作流环境中，数据的处理与上一次的处理相关联，相应的访问控制也如此，因而 TBAC 是一种上下文相关的访问控制模型。其次，TBAC 不仅能对不同工作流实行不同的访问控制策略，而且还能对同一工作流的不同任务实例实行不同的访问控制策略。从这个意义上说，TBAC 是基于任务的，这也表明，TBAC 是一种基于实例（instance-based）的访问控制模型。

TBAC 模型由工作流、授权结构体、受托人集和许可集 4 部分组成。

（1）任务（task）：是工作流程中的一个逻辑单元，是一个可区分的动作，与多个用户相关，也可能包括几个子任务。授权结构体是任务在计算机中进行控制的一个实例。任务中的子任务，对应于授权结构体中的授权步。

（2）授权结构体（authorization unit）：是由一个或多个授权步组成的结构体，它们在逻辑上是联系在一起的。授权结构体分为一般授权结构体和原子授权结构体。一般授权结构体内的授权步依次执行，原子授权结构体内部的每个授权步紧密联系，其中任何一个授权步失败都会导致整个结构体的失败。

（3）授权步（authorization step）：表示一个原始授权处理步，是指在一个工作流程中对处理对象的一次处理过程。授权步是访问控制所能控制的最小单元，由受托人集（trustee-set）和多个许可集（permissions set）组成。

受托人集是可被授予执行授权步的用户的集合，许可集则是受托集的成员被授予授权步时拥有的访问许可。当授权步初始化以后，一个来自受托人集中的成员将被授予授权步，我们称这个受托人为授权步的执行委托者，该受托人执行授权步过程中所需许可的集合称为执行者许可集。授权步之间或授权结构体之间的相互关系称为依赖（dependency），依赖反映了基于任务的访问控制的原则。授权步的状态变化一般自我管理，依据执行的条件而自动变迁状态，但有时也可以由管理员进行调配。

一个工作流的业务流程由多个任务构成。而一个任务对应于一个授权结构体，每个授权结构体由特定的授权步组成。授权结构体之间以及授权步之间通过依赖关系联系在一起。在 TBAC 中，一个授权步的处理可以决定后续授权步对处理对象的操作许可，上述许可集合称为激活许可集。执行者许可集和激活许可集一起称为授权步的保护态。

TBAC 模型一般用五元组（S，O，P，L，AS）来表示，其中 S 表示主体，O 表示客体，P 表示许可，L 表示生命期（lifecycle），AS 表示授权步。由于任务都是有时效性的，所以在基于任务的访问控制中，用户对于授予他的权限的使用也是有时效性的。因

此，若 P 是授权步 AS 所激活的权限，那么 L 则是授权步 AS 的存活期限。在授权步 AS 被激活之前，它的保护态是无效的，其中包含的许可不可使用。当授权步 AS 被触发时，它的委托执行者开始拥有执行者许可集中的权限，同时它的生命期开始倒计时。在生命期期间，五元组（S，O，P，L，AS）有效；生命期终止时，五元组（S，O，P，L，AS）无效，委托执行者所拥有的权限被回收。

TBAC 的访问政策及其内部组件关系一般由系统管理员直接配置。通过授权步的动态权限管理，TBAC 支持最小特权原则和最小泄漏原则，在执行任务时只给用户分配所需的权限，未执行任务或任务终止后用户不再拥有所分配的权限。而且在执行任务过程中，当某一权限不再使用时，授权步自动将该权限回收。另外，对于敏感的任务需要不同的用户执行，这可通过授权步之间的分权依赖实现。

TBAC 从工作流中的任务角度建模，可以依据任务和任务状态的不同，对权限进行动态管理。因此，TBAC 非常适合分布式计算和多点访问控制的信息处理控制以及在工作流、分布式处理和事务管理系统中的决策制定。

4.6.5　基于对象的访问控制模型

DAC 或 MAC 模型的主要任务都是对系统中的访问主体和受控对象进行一维的权限管理，当用户数量多、处理的信息数据量巨大时，用户权限的管理任务将变得十分繁重，并且用户权限难以维护，这就降低了系统的安全性和可靠性。对于海量的数据和差异较大的数据类型，需要用专门的系统和专门的人员加以处理，要是采用 RBAC 模型，安全管理员除了维护用户和角色的关联关系外，还需要将庞大的信息资源访问权限赋予有限个角色。当信息资源的种类增加或减少时，安全管理员必须更新所有角色的访问权限设置，而且，如果受控对象的属性发生变化，同时需要将受控对象不同属性的数据分配给不同的访问主体处理时，安全管理员将不得不增加新的角色，并且还必须更新原来所有角色的访问权限设置以及访问主体的角色分配设置，这样的访问控制需求变化往往是不可预知的，造成访问控制管理的难度和工作量巨大。在这种情况下，有必要引入基于受控对象的访问控制模型（Object-based Access Control Model，OBAC Model）。

控制策略和控制规则是 OBAC 访问控制系统的核心所在，在基于受控对象的访问控制模型中，将访问控制列表与受控对象或受控对象的属性相关联，并将访问控制选项设计成为用户、组或角色及其对应权限的集合。同时，允许对策略和规则进行重用、继承和派生操作。这样，不仅可以对受控对象本身进行访问控制，对受控对象的属性也可以进行访问控制，而且派生对象可以继承父对象的访问控制设置，这对于信息量巨大、信息内容更新变化频繁的管理信息系统非常有益，可以减轻由于信息资源的派生、演化和重组等带来的分配、设定角色权限等的工作量。

OBAC 从信息系统的数据差异变化和用户需求出发，有效地解决了信息数据量大、数据种类繁多、数据更新变化频繁的大型管理信息系统的安全管理。OBAC 从受控对象的角度出发，将访问主体的访问权限直接与受控对象相关联，一方面定义对象的访问控制列表，增、删、修改访问控制项易于操作，另一方面，当受控对象的属性发生改变，或者受控对象发生继承和派生行为时，无须更新访问主体的权限，只需要修改受控对象的相应访问控制项即可，从而减少了访问主体的权限管理，降低了授权数据管理的复杂性。

4.7 VPN 技术

当今，随着企业网应用的日益广泛，企业网的范围也在不断扩大，采用传统的广域网建立企业专网，往往需要租用昂贵的跨地区数字专线。同时，国内公共信息网（ChinaNet 与 Internet）近几年来得到高速发展，已经遍布全国各地。在物理上，各地的公众信息网都是连通的，但由于公众信息网是对社会开放的，如果企业的信息要通过公众信息网进行传输，在安全性上会存在着很多问题。

VPN（Virtual Private Network，虚拟专用网络）是指利用公共网络建立私有专用网络。数据通过安全的“加密隧道”在公共网络中传播，连接在 Internet 上的位于不同地方的两个或多个企业内部网之间建立一条专有的通信线路，就好比是架设了一条专线一样，但是它并不需要真正地去铺设光缆之类的物理线路。VPN 利用公共网络基础设施为企业各部门提供安全的网络互联服务，能够使运行在 VPN 之上的商业应用享有几乎和专用网络同样的安全性、可靠性、优先级别和可管理性。企业只需要租用本地的数据专线，连接上本地的公共信息网，各地的机构就可以互相传递信息。同时，企业还可以利用公共信息网的拨号接入设备，让自己的用户拨号到公众信息网上，就可以安全地连接进入企业网中。使用 VPN 有节省成本、提供远程访问、扩展性强、便于管理和实现全面控制等好处，是目前和今后企业网络发展的趋势。

4.7.1 IPSec

IPSec 协议是 Internet 工程任务组为保证 IP 及其上层协议的安全而制定的一个开放安全标准，IPSec 协议不是一个单独的协议，它给出了应用于 IP 层上网络数据安全的一整套体系结构，包括网络认证头（Authentication Header，AH）协议、封装安全载荷（Encapsulating Security Payload，ESP）协议、密钥管理（Internet Key Exchange，IKE）协议和用于网络认证及加密的一些算法等。IPSec 规定了如何在对等层之间选择安全协议、确定安全算法和密钥交换，向上提供了访问控制、数据源认证和数据加密等网络安全服务。

1．IPSec 协议体系结构

IPSec 协议是 IETF 于 1998 年 11 月公布的 IP 安全标准，IPSec 的设计目的是在

Internet 上建立安全的 IP 连接，用来填补目前 Internet 在安全方面的空白。IPSec 对于 IPv4 是可选的，对于 IPv6 是强制性的。

如图 4-88 所示，IPSec 体系结构的第一个主要的部分是安全结构。IPSec 使用两个协议提供数据包的安全：认证头和封装安全载荷。AH 协议支持访问控制、数据源认证、无连接的完整性和抗重放攻击。ESP 协议提供访问控制、数据机密性、无连接的完整性、抗重放攻击和有限的通信流机密性等安全服务。AH 协议和 ESP 协议都是接入控制的手段，建立在加密密钥的分配和与这些安全协议相关的通信流量管理的基础上。

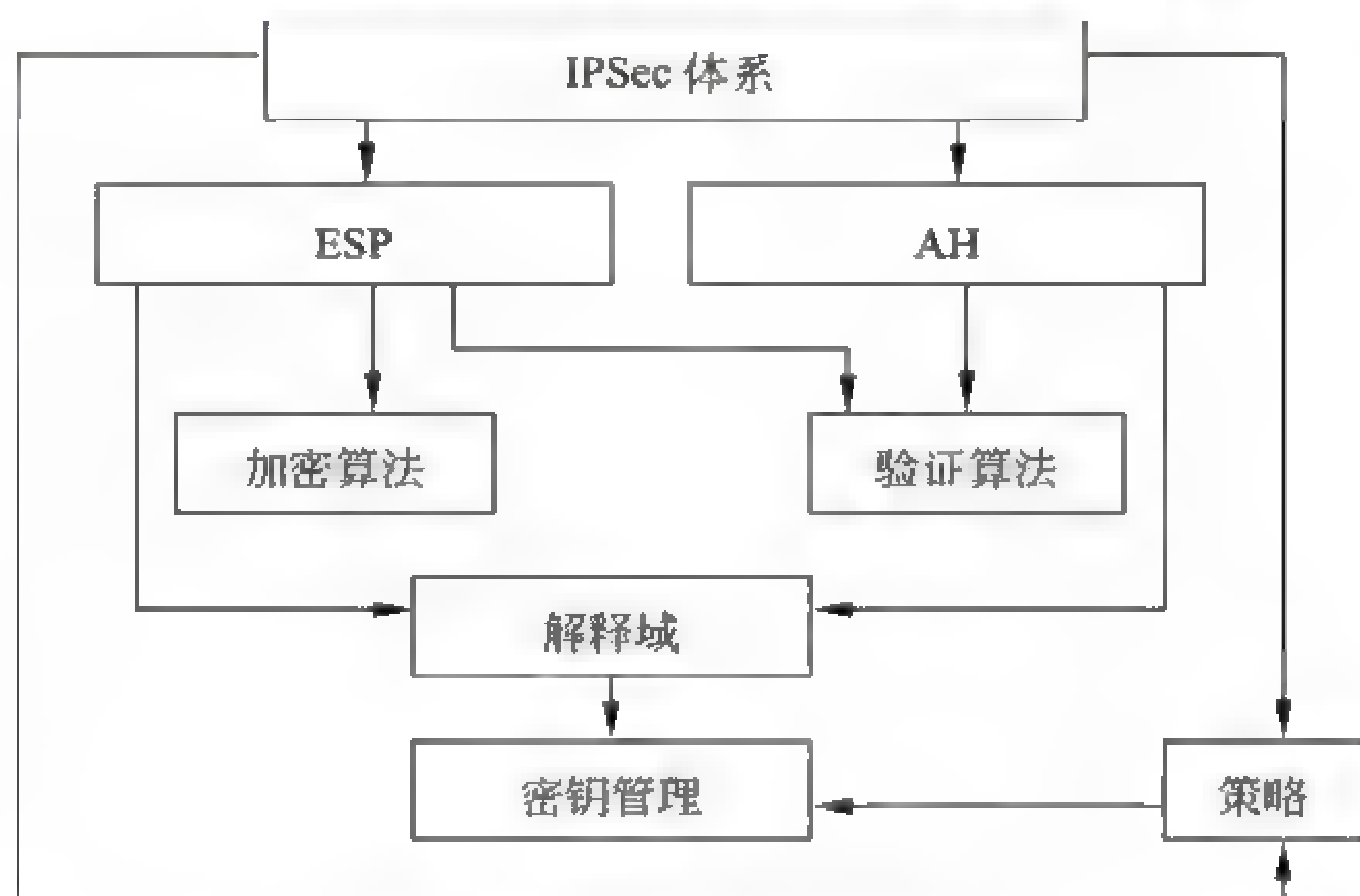


图 4-88　IPSec 体系结构

IPSec 协议使用 IKE 协议实现安全协议的自动安全参数协商。IKE 协商的安全参数包括加密及鉴别算法、加密及鉴别密钥、通信的保护模式（传输或隧道模式）、密钥的生存期等。IKE 还负责这些安全参数的刷新。

解释域（Domain of Interpretation，DOI）是整个 IPSec 协议中很重要的部分，它将所有 IPSec 小组的文献捆绑在一起，通过对解释域的访问可以得到相关协议各字节位的含义解释。它可以被认为是所有的 IPSec 安全参数的主数据库，这些参数可以被与 IPSec 服务相关的系统参考调用。

对于 IPSec 数据流处理而言，有两个必要的数据库：安全关联数据库（Security Association Database，SAD）和安全策略数据库（Security Policy Database，SPD）。SAD 包含活动的 SA 参数；SPD 指定了用于到达或者源自特定主机或者网络的数据流的策略。对于 SPD 和 SAD，都需要单独的输入和输出数据库。

2．安全关联

安全关联（Security Association，SA）是 IPSec 的基础，是两个应用 IPSec 系统（主机、路由器）间的一个单向逻辑连接，是安全策略的具体化和实例化，它提供了保护通信的具体细节。SA 由一个三元组唯一标识，该三元组是：安全参数索引（SPI）、IP 目

的地址和安全协议（AH 或 ESP）标识符。原则上，目的地址可以是一个单播地址、一个 IP 广播地址或一个多播组地址。

安全关联是一个单向“连接”，它为其传输的通信提供安全服务。为了保护两台主机之间双向通信，至少需要两个 SA。若某台主机，如文件服务器或远程访问服务器需要同时与多台客户机通信，则该服务器需要与每台客户机分别建立不同的 SA，每个 SA 用唯一的 SPI 索引标识，当处理接收数据包时，服务器根据 SPI 值来决定该使用哪种 SA。

安全关联数据库是为 IPSec 实现提供安全策略配置，用于维护当前活动的 SA 记录。SAD 中包含现行的 SA 条目，是 SA 的集合，其内容包括目的 IP 地址、安全协议、SPI、序列号计数器和序列号溢出标志。此外，一个 SAD 条目还包括下面几类，分别是算法信息、抗重播窗口、IPSec 协议操作模式和 SA 生存期。

除此之外，SA 中还需要保存其他一些辅助信息，如当前的状态、路径最大传输单元 PMTU 等。SAD 还应该提供其他模块访问自己的接口，最主要的操作就是查找、添加、删除、更新和过期。

3. 安全策略

IPSec 提供的具体服务内容是由系统的安全策略决定的。策略位于安全检查规范的最高一级，是决定系统的安全要素。安全策略定义了系统中哪些行为是允许的，哪些是不允许的。IPSec 协议体系中包括一个安全策略数据库，对安全策略应包括的一些属性进行了概念性的描述，但并没有规定安全策略的具体字段、如何表达等。在实际应用中，用户必须定义一套安全策略，并通过安全策略数据库加以维护，以便为不同的通信指定不同的安全规则。在不同的实施方案中，安全策略往往是造成彼此不能通信的主要原因。进入或外出的每一份数据报，都有三种可能的选择：丢弃、绕过 IPSec 或应用 IPSec。丢弃是指根本不允许离开主机、穿过安全网关，或最终传递到某一应用程序；绕过是指允许通过而不用额外 IPSec 保护的传输；应用是指需要 IPSec 保护传输，并且对于这样的传输 SPD 必须规定提供的安全服务和所使用的协议、算法等。对于一个 IPSec 实施点，进入包和外出包都需要参考 SPD。SPD 包括策略入口的有序列表。每一个策略入口由一个或多个选择符标识，这些选择符定义了被这一策略入口包含的 IP 传输，以及策略或 IPSec 处理的粒度。每一个入口包括一个标识，它标识匹配这一策略的传输是允许通过，丢弃，还是进行 IPSec 处理。如果运用 IPSec 处理，入口应包括 SA 的规范，该规范列举了 IPSec 协议、模式和使用的算法，包括了任何嵌套需求。

4. AH 和 ESP

IPSec 基本协议包括 AH 和 ESP。

1）AH 协议

AH 协议提供数据源认证、数据完整性和反重放保证。AH 的工作原理是在每一个数据包上添加一个身份验证报头。此报头包含一个带密钥的 hash 散列，此 hash 散列在整个数据包中计算，因此对数据的任何更改将致使散列无效，这样就提供了完整性保护。

AH 报头位置在 IP 报头和传输层协议报头之间。AH 由 IP 协议号 51 标识，该值包含在 AH 报头之前的协议报头中，如 IP 报头。AH 可以单独使用，也可以与 ESP 协议结合使用。ESP 协议也提供可选择的认证服务，AH 与 ESP 两者的认证服务的差别在于它们计算时所覆盖的范围不同。

AH 头格式如图 4-89 所示。



图 4-89　AH 头格式

各字段含义如下。

- 下一个报头：是一个 8 位的字段，指明 AH 头之后的载荷类型。字段的值取自于 IANA 的 IP 协议号定义。
- 负荷长度：采用以 32 位的字为单位的值减 2 表示 AH 报头长度。
- 保留：这个 16 位的字段被保留为将来使用，因为目前没有使用，必须将它设为 0。
- 安全参数索引：SPI 是一个任意的 32 位值，被接收者用来识别对进入包进行身份验证的安全关联。它与数据报的目的 IP 地址、安全协议类型一起唯一地确定了这一数据报所用的安全关联。SPI 值 0 被保留来表明“没有安全关联存在”。
- 序号：从 1 开始的 32 位单增序列号，不允许重复，唯一地标识了每一个发送数据包，为安全关联提供反重放保护。接收端校验序列号为该字段值的数据包是否已经被接收过，若是，则拒收该数据包。
- 认证数据：这个字段的长度是可变的，但总是一个 32 位字的整数倍。该认证数据被称为数据报的完整性校验值（ICV）。用来生成 ICV 的算法由 SA 指定。如果一个 IPv4 数据报的 ICV 域的长度不是 32 的整数倍，必须添加填充位使 ICV 域的长度达到所需要的长度。

2）ESP 协议

ESP 提供数据保密、数据源认证、无连接完整性、抗重播服务和有限的数据流保密。实际上，ESP 提供同 AH 类似的服务，但增加了两个额外的服务：数据保密和有限的数据流保密服务。一个 IP 数据报所使用的具体 ESP 服务由相应的安全关联规定。保密服务是 ESP 的主要功能，如果在没有认证的情况下使用保密功能，这个 IP 数据报有可能

受到主动攻击的威胁。数据源认证和完整性认证（统称认证）作为一个整体，是 ESP 的可选用服务。防重放功能仅在有 ESP 认证时生效，并且具体处理取决于报文的接受方。流量保密需要使用 ESP 隧道模式，一般在安全网关处实施，这样可隐藏报文的实际收发地址。

ESP 头格式如图 4-90 所示。



图 4-90　ESP 头的格式

各字段含义如下。

- 安全参数索引：用于标识一个安全关联。
- 序号：单向递增的计数器值，用于防止重放攻击。
- 数据：载荷数据是非定长的域，用来存放经 ESP 协议处理过的数据，这些数据所属的类型由“下一协议头”字段定义。
- 填充字段：额外的字节。有些加密算法要求明文长度是分组的某个整倍数，也可用来隐藏载荷数据的真实长度。
- 填充长度：表示填充的字节数。
- 上层协议：上层协议字段指出了载荷数据所包含的内容。
- 认证数据：长度可变的字段，用于填入 ICV。ICV 的计算范围为 ESP 包中除掉验证数据字段的部分。

5．实施模式

SA 可定义为以下两种模式。

（1）传输模式。传输模式 SA 是两台主机间的一个安全关联。在 IPv4 环境中，传输模式安全协议头紧接在 IP 头和任意选项之后，且在任何更高层协议之前。在 ESP 的情况下，传输模式 SA 仅为那些更高层协议提供安全服务，而并不为 ESP 头之前的 IP 头或任意扩展头提供服务。在 AH 情况下，这种保护也被扩展到 IP 头的可选部分、扩展头的可选部分和可选项。

（2）隧道模式。隧道模式 SA 本质上是一个运用于 IP 隧道的 SA。只要安全关联的任意一端是安全网关，SA 就必须是隧道模式。因此，两个安全网关之间的 SA 总是隧道模式 SA，同样地，主机和安全网关间的 SA 也是这样的。

这两种模式的区别在于通道模式保护整个 IP 数据包，传输模式保护 IP 包内的数据载荷。对应于上面介绍的 AH 协议和 ESP 协议，使用不同的模式，其报文格式有所不同。如图 4-91 和图 4-92 所示。AH 有传输模式和隧道模式两种操作模式。

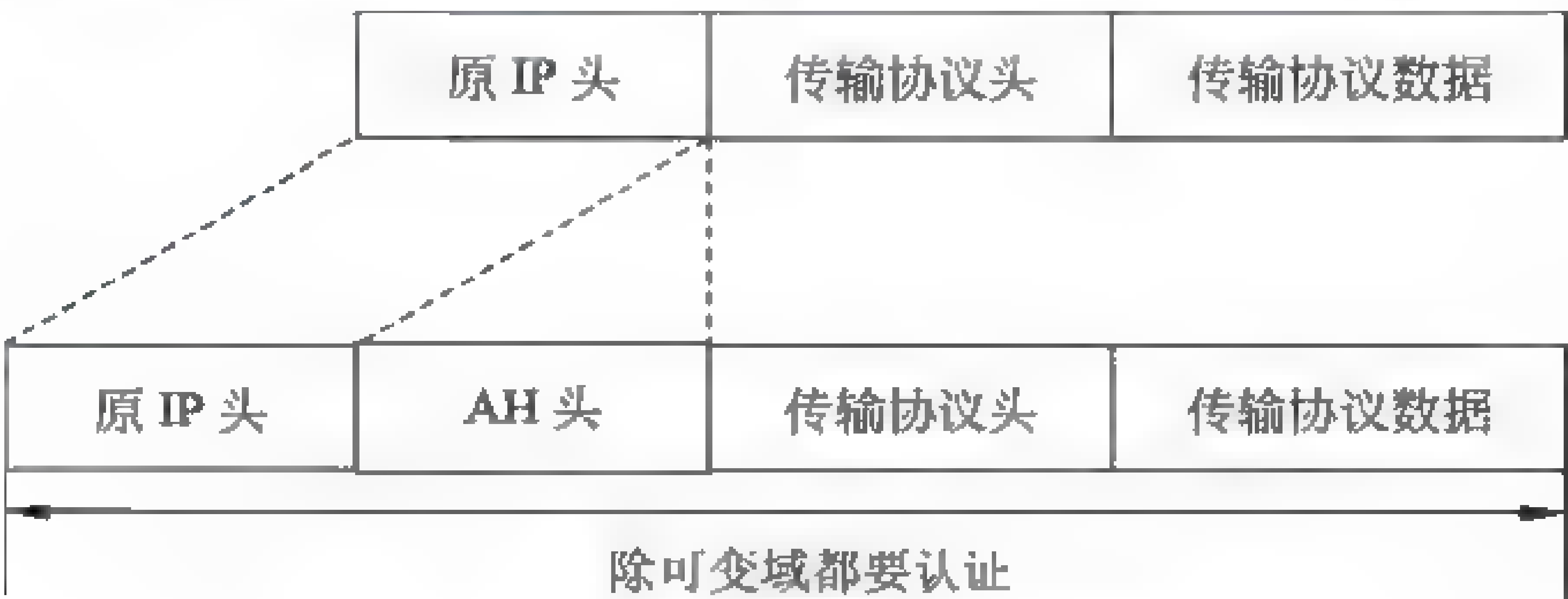


图 4-91　传输模式的 AH 封装

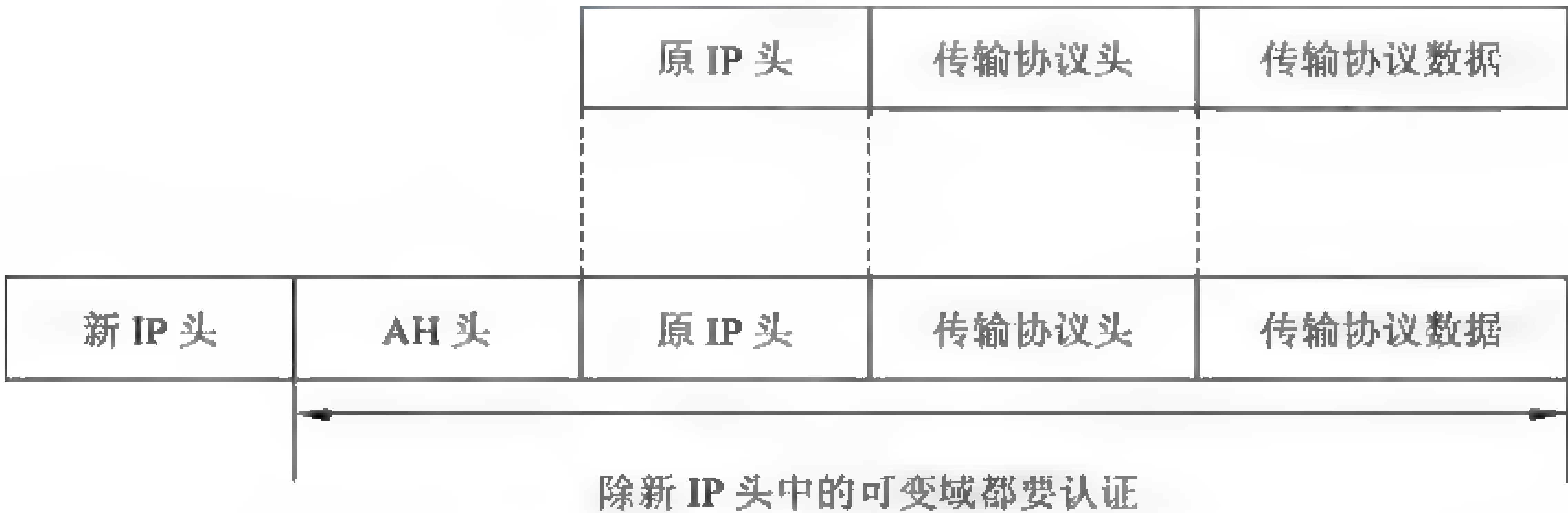


图 4-92　隧道模式的 AH 封装

ESP 协议有两种工作模式，在传输模式中，ESP 协议将上层协议数据作为 ESP 封装的载荷数据，而原 IP 报头仍作为封装后的 IP 分组的报头。在隧道模式中，原 IP 分组被作为载荷数据封装入 ESP，ESP 为封装后的 ESP 载荷构造一个新的 IP 头。

两种模式封装格式如图 4-93 和图 4-94 所示。



图 4-93　传输模式的 ESP 封装

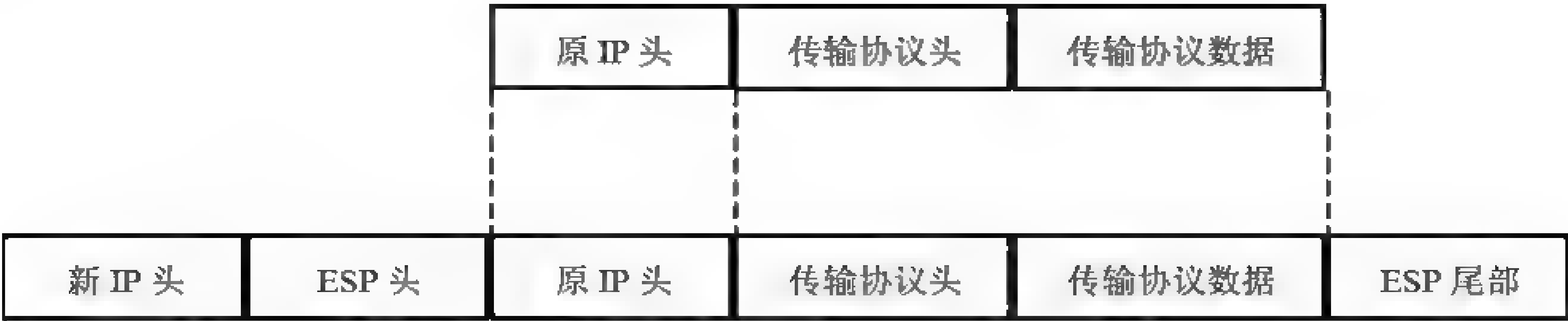


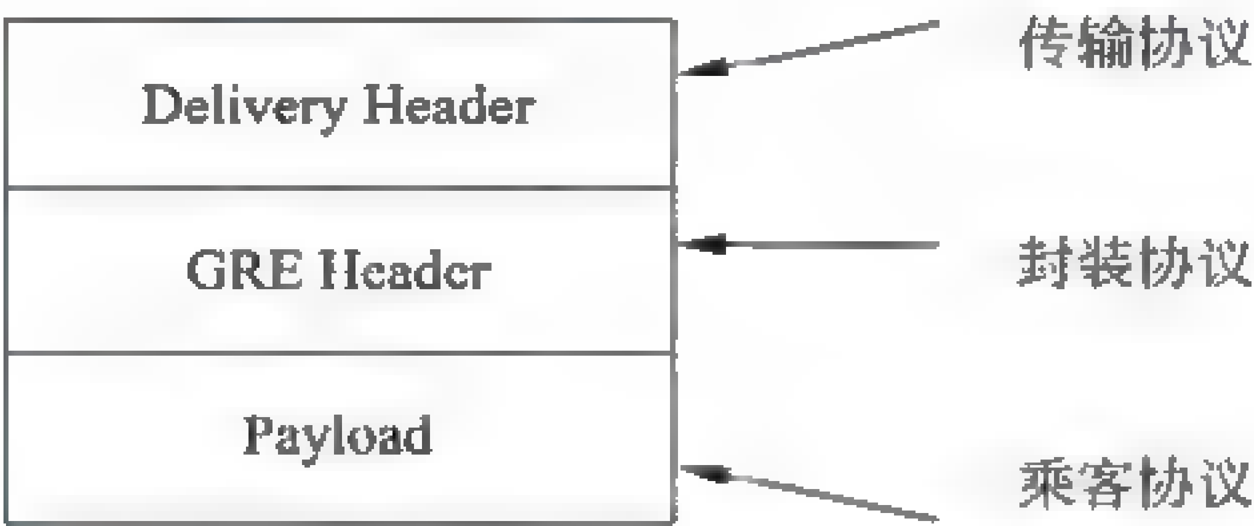
图 4-94　隧道模式的 ESP 封装

4.7.2　GRE

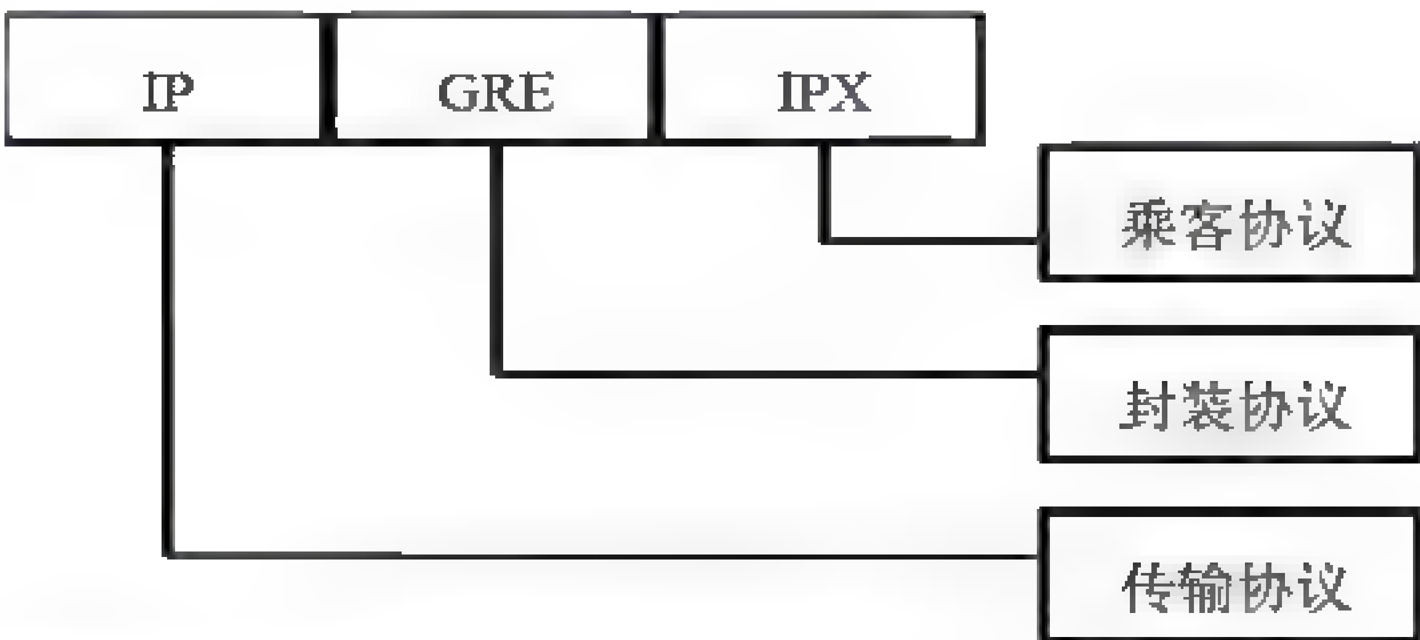
GRE（Generic Routing Encapsulation，通用路由封装）协议是对某些网络层协议（如 IP 和 IPX）的数据报进行封装，使这些被封装的数据报能够在另一个网络层协议中传输。GRE 是 VPN 的第三层隧道协议，同 IPSec 协议一样，GRE 也是在协议层之间采用了 Tunnel（隧道）技术。

1．GRE 报文格式

在最简单的情况下，系统接收到一个需要封装和路由的数据报，我们称之为有效报文（Payload）。这个有效报文首先被 GRE 封装，然后被称之为 GRE 报文，这个报文接着被封装在 IP 报头中，然后完全由 IP 层负责此报文的转发（Forwarded），也称这个负责转发的 IP 协议为传递（Delivery）协议或传输（Transport）协议。整个被封装的报文形式如下。



举例来说，一个封装在 IP tunnel 中的 IPX 传输报文的格式如下。



其中，GRE 报文头的格式如图 4-95 所示。

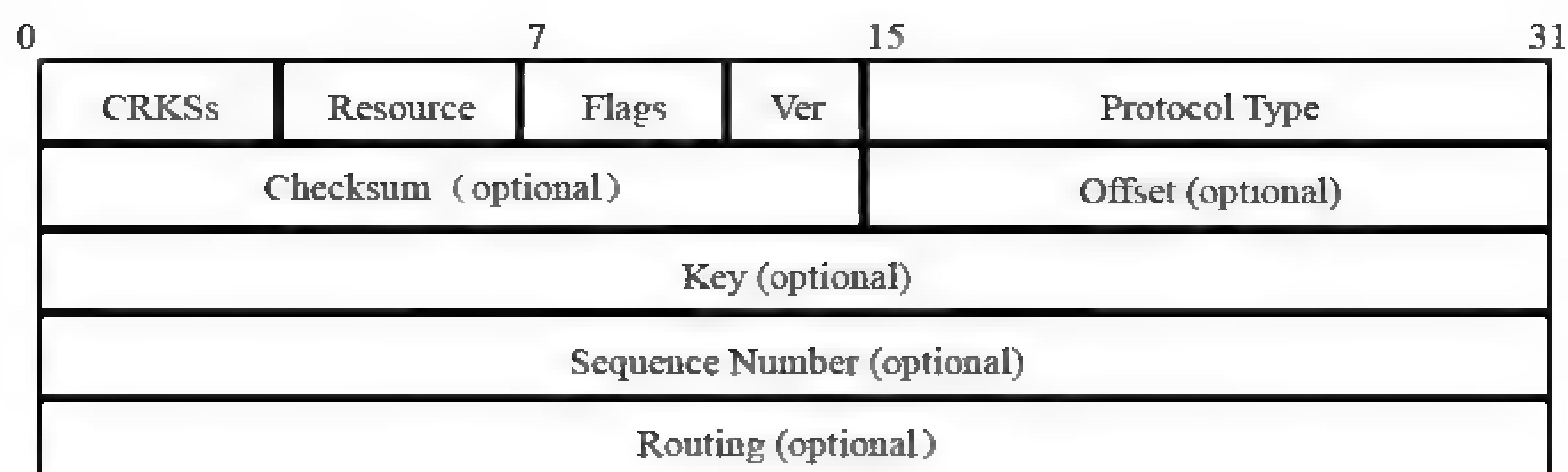


图 4-95　GRE 报文头部格式

下面详细说明各位的含义。

（1）GRE 报头的前 32 位（4 个字节）是必须要有的，构成了 GRE 的基本报头。其中前 16 位上是 GRE 的标记码，其详细说明如下。

- 第 0 位：校验有效位（Checksum Present）。
- 第 1 位：路由有效位（Routing Present）。
- 第 2 位：密钥有效位（Key Present）。
- 第 3 位：顺序号有效位（Sequence Number Present）。
- 第 4 位：严格源路由有效位（Strict Source Route）。
- 第 5 位：递归控制位（Recursion Control）。
- 5～12 位：被保留将来使用，目前必须都被置为 0。
- 13～15 位：保留的版本信息位（Version Number）。

（2）GRE 报头的后 16 位是 Protocol Type（协议类型）字，指明有效数据报的协议类型。最基本的是 IP 协议和以太网协议 IPX，分别对应的协议号为 0x800 和 0x8137。

（3）下面是可选的 GRE 报头区（默认都没有）。

- Checksum（校验信息区）：16 位，包含 GRE 头和有效分组补充的 IP 校验。如果路由有效位或校验有效位有效则此区域有效，而仅当校验位有效时此区域包含有效信息。
- Offset（位移量区）：16 位，表示从路由区开始到活动的被检测的源路由入口（Source Route Entry）的第一个字节的偏移量。如果路由有效位或校验有效位有效则此区域有效，而仅当路由有效位有效时其中的信息有效。
- Key（密钥区）：32 位，包含封装操作插入的 32 位二进制数，它可以被接收者用来证实分组的来源。当密钥位有效时此区域有效。
- Sequence Number（顺序号区）：32 位，包括由封装操作插入的 32 位无符号整数，它可以被接收方用来对那些做了封装操作再传输到接收者的报文建立正确的次序。

（4）最后是长度不定的 Routing（路由）区。

一个完整的 GRE 报文头即由上述的数据格式所构成。

2. GRE 工作过程

因为 GRE 是 Tunnel 接口的一种封装协议，所以要进行 GRE 封装首先必须建立 Tunnel。一旦隧道建立起来，就可以进行 GRE 的加封装和解封装。

（1）加封装过程。首先交由 IPX 模块处理，IPX 模块检查 IPX 包头中的目的地址域确定如何路由此包。如果包的目的地址被发现要路由经过网号为 1f 的网络（为虚拟网号），则将此包发给网号为 1f 的端口即 Tunnel 端口。Tunnel 收到此包后交给 GRE 模块进行封装，GRE 模块封装完成后交由 IP 模块处理，IP 模块做完相应处理后根据此包的目的地址及路由表交由相应的网络接口处理。

（2）解封装的过程。解封装的过程则和上述加封装的过程相反。从 Tunnel 接口收到的报文交给 IP 模块，IP 模块检查此包的目的地址，发现是此路由器后进行相应的处理（和普通的 IP 数据报相同），剥掉 IP 包头然后交给 GRE 模块，GRE 模块进行相应处理后（如检验密钥等），去掉 GRE 包头然后交给 IPX 模块，IPX 模块将此包按照普通的 IPX 数据报处理即可。

3. GRE 的应用

GRE 主要能实现以下几种服务类型。

（1）多协议的本地网通过单一协议的骨干网传输。如图 4-96 所示，Group1 和 Group2 是运行 IPX 协议的本地网，Term1 和 Term2 是运行 IP 协议的本地网。通过在 Router A 和 Router B 之间采用 GRE 协议封装的隧道（Tunnel），Group1 和 Group2、Team1 和 Team2 可以互不影响地进行通信。

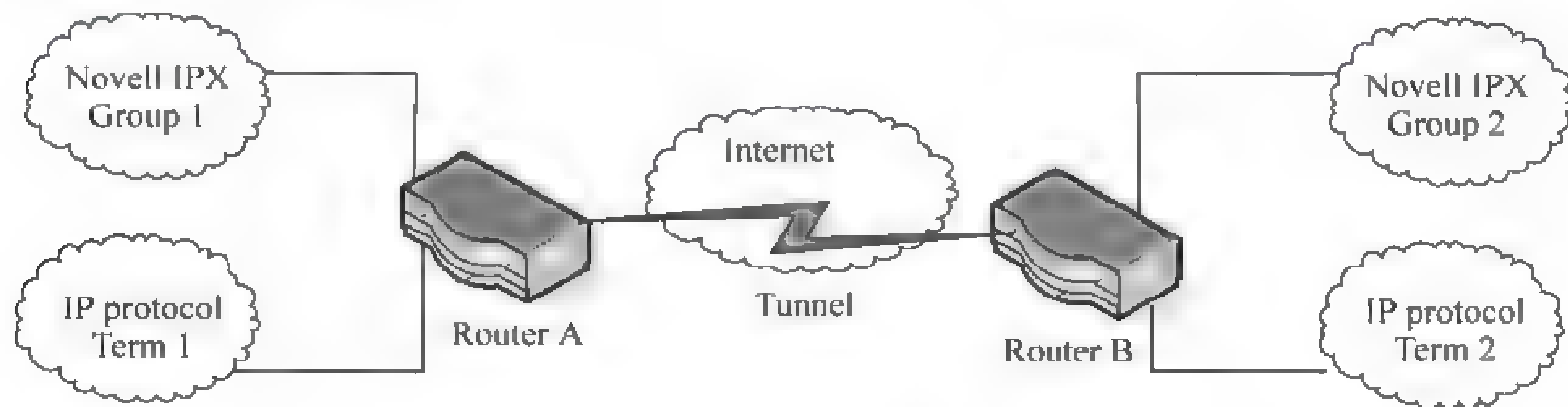


图 4-96 多协议本地网通过单一协议骨干网传输

（2）扩大了步跳数受限协议的网络的工作范围。图 4-97 所示的两台终端之间的步跳数超过 15，它们将无法通信。而通过在网络中使用隧道可以隐藏一部分步跳，从而扩大网络的工作范围。

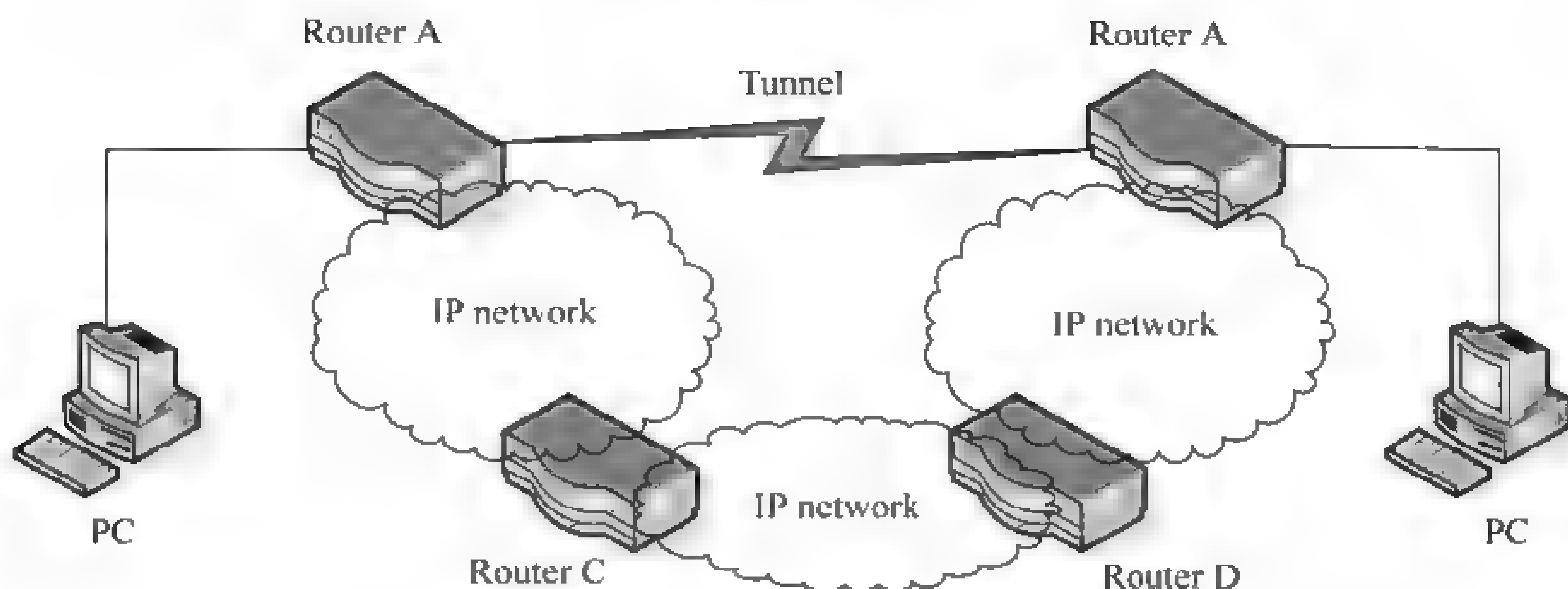


图 4-97　扩大网络工作范围

（3）将一些不能连续的子网连接起来，用于组建 VPN。运行 IPX 协议的两个子网 Group1 和 Group2 分别在不同的城市，通过使用隧道可以实现跨越广域网的 VPN，如图 4-98 所示。

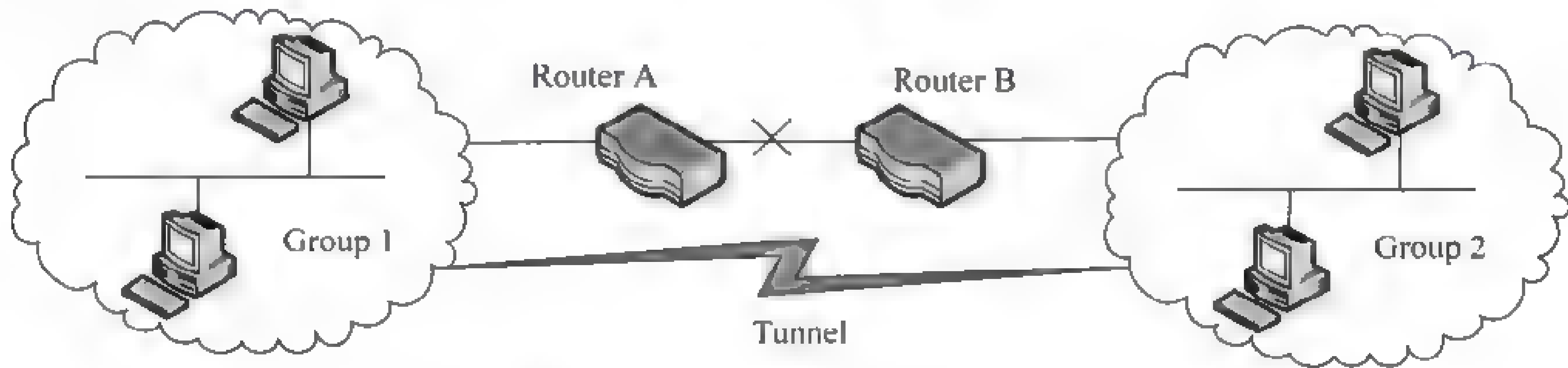


图 4-98　Tunnel 连接不连续子网

（4）与 IPSec 结合使用。对于诸如路由协议、语音和视频等数据先进行 GRE 封装，然后再对封装后的报文进行 IPSec 的加密处理，如图 4-99 所示。

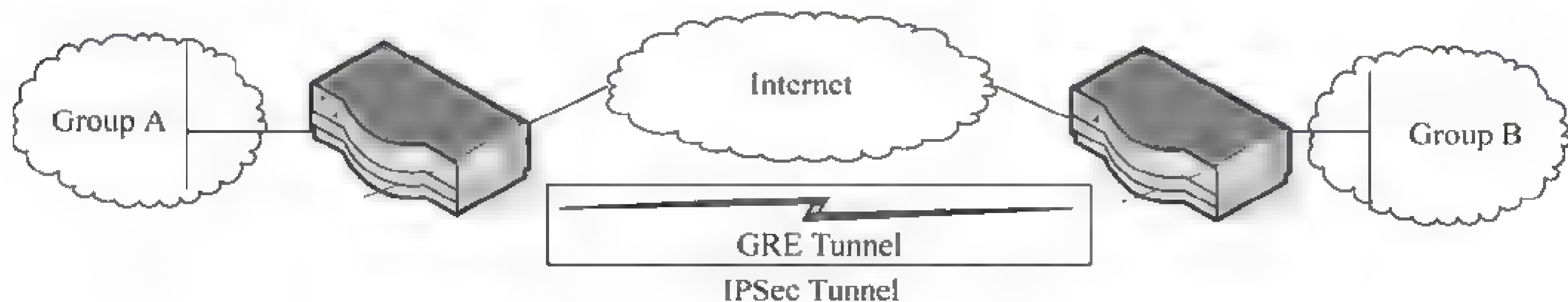


图 4-99　GRE-IPSec 隧道结合

另外，GRE 还支持由用户选择记录 Tunnel 接口的识别关键字，以及对封装的报文进行端到端校验。

由于 GRE 收发双方加封装、解封装处理以及由于封装造成的数据量增加等因素的影响，导致使用 GRE 会造成路由器的数据转发效率有一定程度的下降。

4.7.3 MPLS VPN

基于 MPLS 的 VPN 是 VPN 的一种解决方案。在 MPLS 中，网络供应商为每个 VPN 提供一个唯一的 VPN 标识符（VPN-ID），称之为路由识别符（Route Distinguisher，RD），这个标识符在服务提供商的网络中是独一无二的。转发表中包括一个独一无二的地址，叫做 VPN-IP 地址，是由 RD 和用户的 IP 地址连接形成。每一个 VPN 用户只能与自己的 VPN 网络中的成员进行通信，且只有 VPN 的成员才有权进入该 VPN。

BGP 是一个路由信息分布协议，它利用多协议扩展和共有属性来定义 VPN 的连接性。在基于 MPLS 的 VPN 中，BGP 只对同一个 VPN 的成员发布信息，通过流量分离来提供基本的安全性。因为数据是通过使用 LSP 来转发的，LSP 定义一条不可改变的路径，以保证其安全性。这种基于标签的模式可与帧中继和 ATM 一样提供安全性。这种解决方案的优势在于，服务提供商可以通过相同的网络结构支持多种 VPN，并不需要为每一个用户建立单独的网络。而且，这种方案将 IP VPN 的能力内置于网络本身。所以，服务提供商可以为所有租用者配置一个网络提供专用的 IP 服务，如 Internet 和 Extranet，而无需管理隧道或 VC 机制。服务质量保证可与基于 MPLS 的 VPN 无缝结合，因为两者都是基于标签的技术。基于 MPLS 的 VPN 网络可以很容易地与基于 IP 的用户网络结合起来。租用者可与供应商提供的服务无缝结合，不必改变 Internet 应用，因为这些网络具有通晓性、保密性，且将服务质量内置于网络中，用户能够使用他们专有的 IP 地址而无需网络地址翻译 NAT。

这种网络结构目前可支持多种 VPN，可减轻每一个新网络实施工作的负担。这种方案易于进行 VPN 的添加、移动和改变。如果某个公司需要在自己的 VPN 中增加一个站点，服务提供商只需告诉客户端设备的路由器如何与网络连接，并配置 LSR 识别来自于 PE 的 VPN 成员，BGP 会自动更新 VPN 成员。与增加一台设备需要大量操作的覆盖 VPN 相比，这种方案要简单、迅速且便宜得多。

4.7.4 VPDN

虚拟专用网（Virtual Private Dialup Network，VPDN）是基于拨号用户的虚拟专用拨号网业务，利用 IP 网络的承载功能，结合相应的认证和授权机制，可以建立安全的虚拟专用网络。

随着全球范围内因特网的迅速发展，电子商务的应用正变得越来越广泛，各种企业用户远程办公的需求日益增强，用户发现单靠自己很难构造和维护一个能满足不断增强需求的企业网络，而利用因特网的优势建设一个网络部署灵活简便、一次性投资较小、管理和维护成本低的 VPDN 能很好地满足用户的这类需求。它使企业网络几乎可以无限

延伸到每个角落，从而以安全、低廉的网络互联模式为应用服务提供发展的舞台。

通过使用 VPDN 业务，企业出差人员可以远程经过公共 IP 网络，通过虚拟的加密通道与企业内部的网络连接，而公共网络上的用户则无法穿过虚拟通道访问该企业的内部网络，如图 4-100 所示。

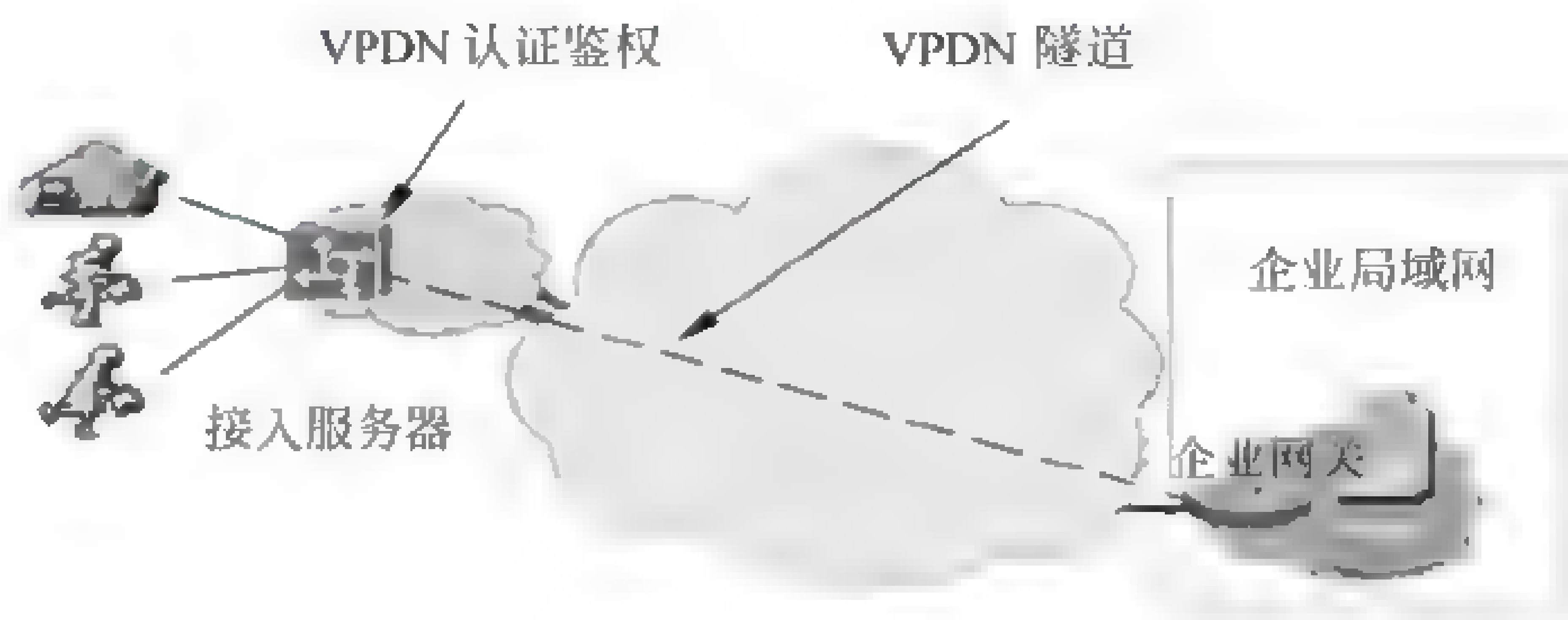


图 4-100　VPDN 功能模块示意图

使用 VPDN 进行远程访问，可以节约昂贵的长途电话费；可以大大节约链路租用费、设备购置费以及网络维护费，减少企业的运营成本。除此之外，更能将 Internet、企业内部网络（Intranet）、企业外部网络（Extranet）及远程接入功能（Remote Access）整合于同一条对外线路中，不需要像以前那样，同时管理 Internet 专线、长途数据专线等多种不同线路。企业可以利用无处不在的 Internet 通过单一网络结构为职员和商业伙伴提供无缝和安全的连接；基于 VPDN 的 Extranet 能加强与用户、商业伙伴和供应商的联系；用户只需与服务提供商签约，将各网络节点接入公用网络，并对网络进行相关配置即可。企业可以迅速构建一个属于自己的专用网络，增进工作效率与员工生产力，提高企业整体的竞争力。VPDN 是逻辑上的网络，用户要扩大或改变 VPDN 覆盖范围只需再签约、进行相应的软件操作即可。VPDN 利用隧道技术，通过在公用网络上建立逻辑隧道、网络层的加密以及采用口令保护、身份验证、权限设置、防火墙等措施，保证数据的完整性，避免被非法窃取。

1．VPDN 的技术介绍

VPDN 有如下三层含义。

（1）VPDN 是虚拟的网络，即没有固定的物理连接，网路只有用户需要时才建立。“虚拟”的概念是相对传统私人专用网络的构建方式而言的，对于广域网连接，传统的组网方式是通过远程拨号和专线连接来实现的，而 VPN 是利用服务提供商所提供的公共网络来实现远程的广域连接。

（2）VPDN 是利用公众网络设施构成的专用网，构建在这些公共网络上的 VPN 将像当前企业私有的网络一样提供安全性、可靠性和可管理性等。

（3）VPDN 是基于拨号用户的，不是所有宽带、局域网上网方式都能支持连接。

当VPDN用户拨号NSP（网络服务提供商）的网络访问服务器NAS（Network Access Server），发出PPP连接请求，NAS收到呼叫后，在用户和NAS之间建立PPP链路，然后，NAS对用户进行身份验证，确定是合法用户，就启动VPDN功能，与公司总部内部连接，访问其内部资源。拨号服务器与公司的企业网关之间直接建立tunnel，在此过程中用户的数据如IPX、IP等协议，经过系列封装，通过tunnel传递到企业网关，再进行解包，传递到企业内部。

VPDN结构示意图如图4-101所示。



图4-101　VPDN结构示意图

VPDN的技术核心主要在于隧道技术和安全技术，网络隧道技术指的是利用一种网络协议来传输另一种网络协议，它主要利用网络隧道协议来实现这种功能。

主要的节点设备如下。

（1）用户端设备（Customer Premises Equipment，CPE）：用户端需具备作为VPDN的网关功能的设备，它位于用户总部，可以由企业网内部的路由器实现，具体可以选用同时具备路由功能和VPDN功能的网络设备。

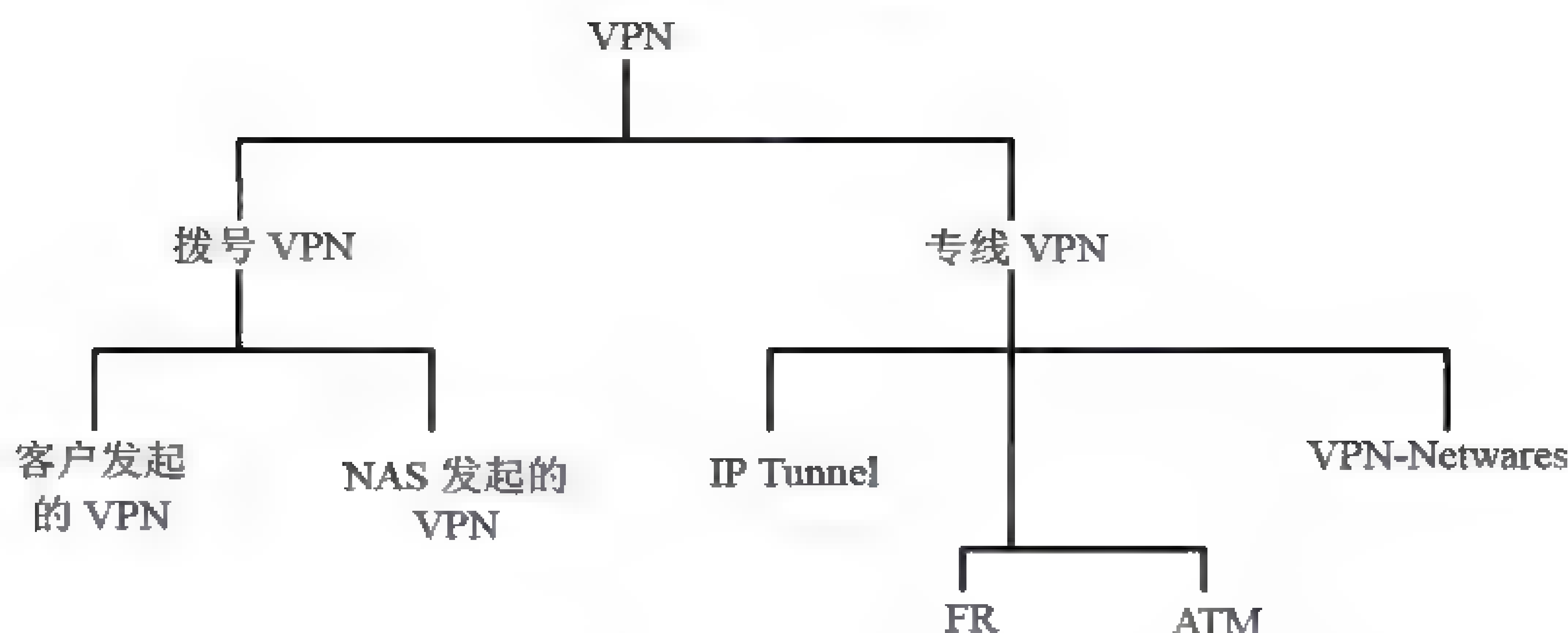
（2）接入服务器（Network Access Server，NAS）：NAS由网络运营商如联通公司提供并承担运维工作，其作用是作为VPDN的接入服务器，可以提供广域网接口，负责与企业专用网的VPN连接，并支持各种LAN局域网协议，支持安全管理和认证，支持隧道及相关技术。

（3）用户终端：用户需具备能使用CDMA1X上网的终端设备，在目前，可以使用的方式包括CDMA1X无线上网卡、CDMA1X手机连接笔记本式计算机及CDMA1X手机连接台式计算机等。

（4）用户端认证服务器：用户端认证服务器是可选的设备，用于对登录用户做鉴权认证。为了便于对用户的账户密码资料进行管理，一般情况下建议设置。

2．VPDN的分类

VPN可以分为拨号VPN和专线VPN。而拨号VPN又可分为客户发起的（Client-Initiated）VPDN和NAS发起的VPDN。



1）客户发起的 VPDN

在客户发起的 VPDN 中，用户拨号到本地的 POP 远程，由客户来发出请求并建立到某企业内部网的加密隧道。为了建立一个安全的连接，客户端运行 IPSec 软件，客户软件与公司内部网络防火墙上的 IPSec 进程通信，或者直接与支持 IPSec 的路由器通信，确保连接的安全性。

这种形式的 VPDN 优点是:远程用户能够同时与多个 Home Gateway 建立 IP Tunnel。远程用户不必重新拨号，就可以进入另一网络。VPDN 的建立和管理与 ISP 无关。

缺点是：因为这种加密的 VPDN 隧道对于服务提供商而言是透明的，在客户端需要专用的拨号软件，而且管理移动 PC 上的 IPSec 客户端软件也是麻烦的事件。

2）NAS 发起的 VPDN

在 NAS 发起的 VPDN 中，由服务提供商的 POP 中的 NAS 请求并创建到客户公司路由器(或者 Home Gateway)的 VPDN 隧道。NAS 使用 L2F(Layer 2 Forwarding Protocol)或者 L2TP（Layer 2 Tunneling Protocol）协议来建立到客户 Home Gateway 的安全隧道。L2TP 是不久前建立的标准,这个标准结合了 Cisco 公司的 L2F 和微软公司的 PPTP 协议。对于 Home Gateway 来说,L2F 或 L2TP 隧道表现得似乎是用户直接拨号到公司内部网上。

在这种拨号 VPDN 形式中，用户认证分两级处理。当用户拨入时，首先由服务提供商 NAS 执行基本的认证，这个认证仅仅识别出用户的公司身份。然后，NAS 打开到用户公司 Home Gateway 的隧道，由 Home Gateway 来执行用户级的认证功能。

这种 VPDN 形式有若干优点：对拨号用户透明，用户 PC 上无需特殊的客户软件，因而管理简单化；由于是由服务提供商初始化隧道，他们可以提供优质的拨号 VPDN 服务，如通过预留 Modem 端口、优先的数据传送等手段保证拨号 VPDN 用户得到所需的服务；NAS 可以支持 Internet 或其他公用网络和 VPDN 服务；由于到某一目的的通信量全部通过单一隧道传送，大规模部署将更具有可扩充性和管理性。

这种 VPDN 形式存在的缺点有：当远程用户进入其他网络时，需要重新拨号，并且只能以另一用户名登录；远程用户不能同时进入多个网络。

4.8 企业网络安全隔离

4.8.1 网络隔离技术概述

网络隔离（Network Isolation）技术的目标是确保把有害的攻击隔离，在可信网络之外和保证可信网络内部信息不外泄的前提下，完成网间数据的安全交换。有多种形式的网络隔离，如物理隔离、协议隔离和 VPN 隔离等。无论采用什么形式的网络隔离，其实质都是数据或信息的隔离。网络隔离的重点是物理隔离。物理隔离的一个特征，就是内网与外网永不连接，内网和外网在同一时间最多只有一个同隔离设备建立非 TCP/IP 协议的数据连接。

把网络与非安全区域划开，就如同在城市周围挖一条护城河，然后再建几个可以控制的“吊桥”，保持与城外的互通。网络隔离的重要内容之一就是研究“桥”上的防护技术。目前有以下几种策略。

（1）修桥策略。业务协议直接通过，数据不重组，对速度影响小，安全性弱。例如，防火墙完成网络层的过滤，而多重安全网关完成从网络层到应用层的过滤，实现多重关卡策略。

（2）渡船策略。业务协议不直接通过，数据要重组，安全性比较好。例如，网闸采用协议落地，安全检测依赖于现有安全技术，而交换网络通过建立交换缓冲区实现立体化安全监控与防护。

（3）人工策略。不做物理连接，人工用移动介质交换数据，安全性较好。

不同的业务网络根据自己的安全需求，选择不同的网络隔离技术，主要是看数据交换的量大小、实时性要求、业务服务方式的要求。表 4-10 给出了不同的网络隔离技术的比较。

表 4-10 不同的网络隔离技术的比较

网络隔离技术	安 全 性	适 合 场 合
人工方式	安全性最好，物理隔离	适合临时的小数量的数据交换
数据交换网	物理上连接，采用完整安全保障体系的深层次防护（防护、监控、审计），安全程度依赖当前安全技术	适合提供大数据服务或实时的网络服务，支持多业务平台建设
网闸	物理上不同时连接，对攻击防护好，但协议的代理对病毒防护依赖当前技术	适合定期的批量数据交换，但不适合多应用的穿透
多重安全网关	从网络层到应用层的防护	不适合涉密网络与非涉密网络数据交换。适合办公网络与因特网的隔离，也适合涉密网络之间的隔离
防火墙	网络层的安全防护	适合网络的安全区域的隔离，适合同安全级别的网络隔离

4.8.2　划分子网隔离

在工程实践中，子网划分是进行网络隔离的常用方法，但进行子网划分不仅仅是为了网络隔离，可能是为了减轻系统的拥挤状况、方便使用多种媒体介质、方便查找网络错误，或者限制广播信息传播范围等。例如，网络上的两个节点进行通信时占用了整个网络系统的带宽，当增加节点时就需要补充新的带宽。如果将通信活动比较频繁的节点分放在各自的子网中，就可减少一个网络上通信节点的数目，使得各节点在较小的网络内部相互通信，从而减轻系统的拥挤程度。再如，要将分布在较广范围内的所有节点，通过同种介质连接成一个单一的网络，不仅不方便，而且造价太高，有时甚至是不可能的。应根据具体情况，先采用多种介质将各个节点连成不同的子网，然后再互连成一个较大的网络。此外，利用子网划分可以减轻 CPU 的负载。在一个较大的网络上，过多的节点数目可能会导致网上广播信息太多，即使某个广播数据不是发送给某个节点的，网中每个节点在决定是否接收其之前，仍要处理该数据报，这样就加重了连接到网上各节点 CPU 的负载。

从网络安全的角度，划分子网在保证系统的安全性和限制网络错误的范围等方面也非常重要。在一个较大的网络中，每一个节点都能访问发送到网络上的所有数据报。若将一个较大的校园网划分成若干个子网，可将一些敏感的、需要保密的信息限制在某一个子网内，以限制其他子网或网段上节点对其访问。此外，通过将覆盖范围较大的校园网划分成若干个子网，也可将一些对整个网络影响比较大的网络错误限制在很小的范围。

子网划分通常是由本地网络根据子网屏蔽字来进行的。子网屏蔽字是一个 32 位的数字，其中所有的 1 表示 IP 地址中的网络地址段和子网地址段，所有的 0 表示 IP 地址中的主机地址段。子网的划分要在考虑诸多因素的条件下作出满足实际要求和未来发展需要的方案，如网络地址、数据流量和安全控制分域、行政体制、地理分布等。

划分子网的互连和隔离可采用下列方法。

（1）路由器是网络层互连设备，具有子网互连和隔离的作用，且在网络安全、网络管理和故障隔离等方面也起着极为重要的作用。采用路由器既可实现各子网的互连，也可实现校园网与外部其他网络的互连。

（2）采用交换式集线器实现主干网与各局域网的互连，这种集线器含有高速背板，用以连接各种接口和功能模块，可将各个局域网以桥接方式或路由方式挂接到主干网上，其性能保证了本身不会成为网络瓶颈，而且能起到各网段或子网之间的隔离作用。同时还提供了一种非常灵活的网络控制手段，例如地址过滤、转发设定和网络结构控制等。

（3）工程实践中的网络应具有可伸缩性，以适应网络物理结构和有关业务的变化，而网络的可伸缩性和网络的虚拟能力密切相关，所以在网络互连时要尽量采用具有虚拟化能力的互连设备。网络的虚拟能力可使一个用户从一个逻辑子网很方便地转移到另一个逻辑子网内，而不受其所在物理位置的限制。

（4）在结构化布线的基础上采用结构化网络设计，使网络尽量呈现出一种星型或树型结构。这样便于子网的互连以及网络的拓展，有利于网络的管理和维护。若再增加一些可靠性措施，如故障隔离等，可进一步提高网络的可靠性。

4.8.3 VLAN 隔离

1．VLAN 隔离的概念

VLAN 是一种划分相互隔离子网的技术，通过将网内设备逻辑地而不是物理地划分成一个个网段从而实现虚拟工作组。VLAN 一方面为了避免当一个网络系统的设备数量增加到一定规模后，大量的广播报文消耗大量的网络带宽，从而影响有效数据的传递；另一方面确保部分安全性比较敏感的部门不被随意访问浏览。此外，VLAN 能够形成虚拟工作组，动态管理网络。1999 年，IEEE 颁布了用以标准化 VLAN 实现方案的 802.1Q 协议标准草案。

2．VLAN 隔离的作用和优点

通过 VLAN 隔离技术，可以把一个网络系统中众多的网络设备分成若干个虚拟的工作组，组和组之间的网络设备在二层上相互隔离，形成不同的广播域，将广播流量限制在不同的广播域。由于 VLAN 技术是基于二层和三层之间的隔离，可以将不同的网络用户与网络资源进行分组并通过支持 VLAN 技术的交换机隔离不同组内网络设备间的数据交换来达到网络安全的目的。该方式允许同一 VLAN 上的用户互相通信，而处于不同 VLAN 的用户之间在数据链路层上是断开的，只能通过三层路由器才能访问。

使用 VLAN 隔离技术也有一个明显的缺点，那就是要求网络管理员必须明确交换机的每一个物理端口上所连接的设备的 MAC 地址或者 IP 地址，根据需求划分不同的工作组并对交换机进行配置。当某一网络终端的网卡、IP 地址或是物理位置发生变化时，需要对整个网络系统中多个相关的网络设备进行重新配置，这加重了网络管理员的维护工作量，所以也只适用于小型网络。

VLAN 隔离技术具有如下优点。

（1）增加了网络的连接灵活性。借助 VLAN 技术，能将不同地点、不同网络、不同用户组合在一起，形成一个虚拟的网络环境，就像使用本地 LAN 一样方便、灵活、有效。VLAN 可以降低移动或变更工作站地理位置的管理费用，特别是一些业务情况有经常性变动的公司使用了 VLAN 后，这部分管理费用大大降低。

（2）控制网络上的安全。VLAN 可以提供建立防火墙的机制，防止交换网络的过量广播。使用 VLAN，可以将某个交换端口或用户赋予某一个特定的 VLAN 组，该 VLAN 组可以在一个交换网中或跨接多个交换机，在一个 VLAN 中的广播不会送到 VLAN 之外。同样，相邻的端口不会收到其他 VLAN 产生的广播。这样可以减少广播流量，释放带宽给用户应用，减少广播的产生。

（3）增加网络的安全性。因为一个 VLAN 就是一个单独的广播域，VLAN 之间相互

隔离，这大大提高了网络的利用率，确保了网络的安全保密性。人们在 LAN 上经常传送一些保密的、关键性的数据。保密的数据应提供访问控制等安全手段。一个有效和容易实现的方法是将网络分段成几个不同的广播组，网络管理员限制了 VLAN 中用户的数量，禁止未经允许而访问 VLAN 中的应用。交换端口可以基于应用类型和访问特权来进行分组，被限制的应用程序和资源一般置于安全性 VLAN 中。

3. VLAN 隔离技术的分类

VLAN 隔离技术可分为基于端口的 VLAN、基于 MAC 地址的 VLAN、基于第三层的 VLAN 和基于策略的 VLAN。

（1）基于端口的 VLAN。基于端口的 VLAN（如图 4-102）是划分虚拟局域网最简单也是最有效的方法，这实际上是某些交换端口的集合，网络管理员只需要管理和配置交换端口，而不管交换端口连接什么设备。

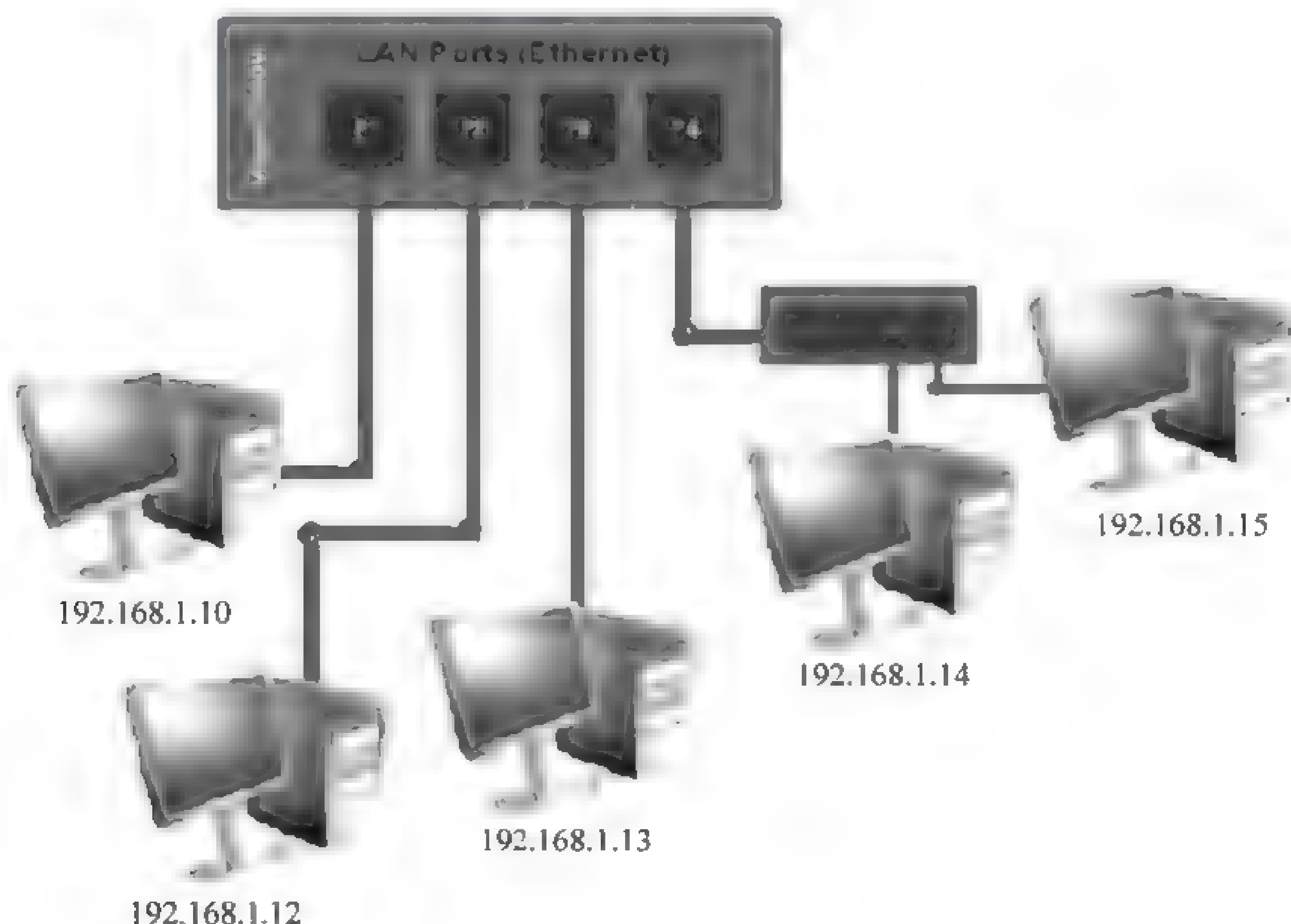


图 4-102　基于端口的 VLAN 划分

（2）基于 MAC 地址的 VLAN。由于只有网卡才分配有 MAC 地址，因此按 MAC 地址来划分 VLAN 实际上是将某些工作站和服务器划属于某个 VLAN。事实上，该 VLAN 是一些 MAC 地址的集合。当设备移动时，VLAN 能够自动识别。网络管理需要管理和配置设备的 MAC 地址，显然当网络规模很大，设备很多时，会给管理带来难度。

（3）基于第 3 层的 VLAN。基于第 3 层的 VLAN 是采用在路由器中常用的方法，如 IP 子网和 IPX 网络号等。其中，局域网交换机允许一个子网扩展到多个局域网交换端口，

甚至允许一个端口对应于多个子网。

（4）基于策略的 VLAN。基于策略的 VLAN 是一种比较灵活有效的 VLAN 划分方法。常用的策略往往与厂商设备的支持有关，如按 MAC 地址、IP 地址、以太网协议类型和网络的应用等。

4. VLAN 隔离技术的应用

在同一个 VLAN 中的工作站，不论它们实际与哪个交换机连接，它们之间的通信就好像在独立的集线器上一样。同一个 VLAN 中的广播只有 VLAN 中的成员才能听到，而不会传输到其他的 VLAN 中去，这样可以很好地控制不必要的广播风暴的产生。同时，若没有路由，不同 VLAN 之间不能相互通信，这样增加了企业网络中不同部门之间的安全性。网络管理员可以通过配置 VLAN 之间的路由来全面管理企业内部不同管理单元之间的信息互访。交换机根据用户工作站的 MAC 地址来划分 VLAN，所以，用户可以自由地在企业网络中移动办公，不论他在何处接入交换网络，都可以与 VLAN 内其他用户自如地通信。

目前，基于 VLAN 隔离技术的访问控制方法在一些中小型企业和校园网中得到广泛的应用。

在安全性方面，VLAN 隔离技术可以保证物理设备之间的隔离，但是对于同一台服务器，只能做到同时向多个 VLAN 组全面开放或者是只向某个 VLAN 组开放，而不能针对个别用户进行限制。在实际应用中，一台服务器担当多种服务器角色，同时为多个 VLAN 组用户提供不同的服务，这也带来一定的安全隐患。

例如，一台市场部电子商务服务器存储有客户数据，同时它也是一台财务部数据库服务器，存储有财务数据，这样该服务器就同时需要向市场人员和财务人员开放，单纯地采用 VLAN 技术就无法避免市场人员查看财务数据，当然，这种隐患可以通过其他辅助手段解决。

4.8.4 逻辑隔离

1. 防火墙

防火墙是通过提供访问控制服务来实现对内部网络的安全防护的，它已经在 Internet 上得到了广泛的应用，但它只是网络安全策略中的一个组成部分。防火墙技术不仅可融入加密传输技术和认证技术，而且可结合安全协议，以提供更高的网络安全性。防火墙是一种网络安全设施，是执行访问控制策略的一个或一组软、硬件系统。其主要手段是通过放置于网络拓扑结构的合适节点上，使其成为内外通信的唯一途径，从而隔离内部和外部网络。并按照根据安全策略制定的过滤规则（访问控制规则）对经过它的信息流进行监控和审查，过滤掉任何不符合安全规则的信息，以保护内部网络不受外界的非法访问和攻击。防火墙是一种建立在被认为是安全可信的内部网络和被认为是不太安全可信的外部网络（Internet）之间的访问控制机制，是安全策略的具体体现。

2. 多重安全网关

防火墙是在“桥”上架设的一道关卡，只能做到类似“护照”的检查；多重安全网关的方法就是架设多道关卡，有检查行李的、有检查人的。多重安全网关也称为 UTM（统一威胁管理），实现从网络层到应用层的全面检查。

多重安全网关的检查分为如下几个层次。

（1）FW：网络层的 ACL。

（2）IPS：防入侵行为。

（3）AV：防病毒入侵。

（4）可扩充功能：自身防 DoS 攻击、内容过滤和流量整形等。

多重安全网关提供了完全性安全保护。这种技术对 OSI 七层模型中描述的所有层次的内容进行处理，其有效性超过了状态检测技术以及深度包检测技术，具备在千兆网络环境中，实时将网络层数据负载重组为应用层对象的能力，而且重组之后的应用层对象可以通过动态更新病毒和蠕虫特征来进行扫描和分析。多重安全网关还可探测其他各种威胁，包括不良 Web 内容、垃圾邮件、间谍软件和网络钓鱼欺骗。多重安全网关通常需要应用 ASIC 技术来获得性能保证。ASIC 芯片是多重安全网关的一个关键组成部分。为了提供千兆级实时的应用层安全服务的平台，专门为网络骨干和边界上高性能内容处理设计的体系结构是必不可少的。ASIC 芯片集成了硬件扫描引擎、硬件加密和实时内容分析处理能力，提供防火墙、加密/解密，特征匹配和启发式数据包扫描以及流量整形的加速功能。在软件组件方面，多重安全网关使用专用的经过定制的操作系统。专用的强化安全的操作系统提供精简的、高性能防火墙和内容安全检测平台。基于内容处理加速模块的硬件加速，加上智能排队和管道管理，使各种类型流量的处理时间达到最小，从而实时有效地实现防病毒、防火墙、VPN、反垃圾邮件和 IDP 等功能。此外，基于防火墙等产品的经验，多重安全网关在规则算法、模式识别语言等方面一般也有特别的设计。

与防火墙比较，多重安全网关也是采用“架桥”的策略，主要是采用安全检查的方式，不更改应用协议，所以速度快，流量大，从客户应用上来看则没有不同。

3. 交换网络

交换网络的模型来源于银行系统的 Clark-Wilson 模型，主要是通过业务代理与双人审计的思路保护数据的完整性。交换网络是在两个隔离的网络之间建立一个网络交换区域，负责数据的交换。交换网络的两端可以采用多重网关，也可以采用网闸。在交换网络内部采用监控、审计等安全技术，整体上形成一个立体的交换网安全防护体系。交换网络示意图如图 4-103 所示。

交换网络的核心也是业务代理，客户业务要经过接入缓冲区的申请代理，到业务缓冲区的业务代理，才能进入生产网络。

交换网络技术和网闸一样，都是采用渡船策略，延长数据通信“里程”，增加安全保障措施。

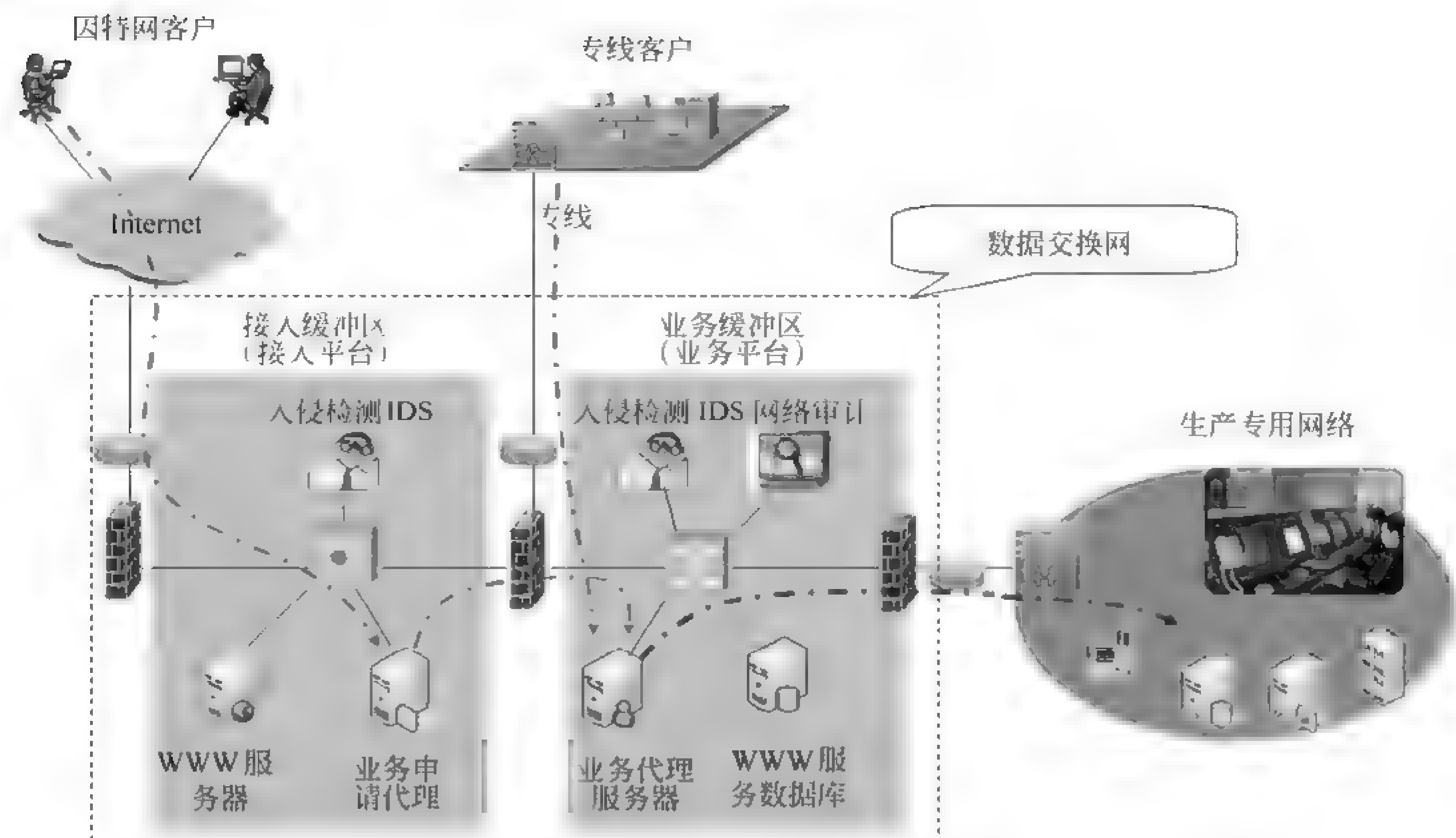


图 4-103　交换网络示意图

4.8.5　物理隔离

1．物理隔离的概念

在实行物理隔离之前，网络的信息安全有许多措施，如在网络中增加防火墙、防病毒系统，对网络入侵检测、漏洞扫描等。由于这些技术的极端复杂性与有限性，这些在线分析技术无法提供某些机构（如军事、政府和金融等）需要的高度数据安全要求。而且，此类基于软件的保护是一种逻辑机制，对于逻辑实体而言极易被操纵。特别是涉密网不能把机密数据的安全完全寄托在用概率来作判断的防护上，必须有一道绝对安全的大门，保证涉密网的信息不被泄露和破坏。不仅国内涉密网络的安全保密防护非常薄弱，即使是美国军方也分别在 20 世纪 80 年代和 1999 年 11 月两次明确地要求物理隔离。Internet 前身实际是美国一个军方网，在发现大量的攻击后，曾经大规模地断开了一些时间。我国国家保密局于 1999 年 12 月 27 日发布了物理隔离要求，2000 年 1 月 1 日起颁布实施了《计算机信息系统国际联网保密管理规定》，其中第二章保密制度第六条规定："涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其他公共信息网络相连接，必须实行物理隔离。"

物理隔离的原理是：每一次数据交换，物理隔离都经历了数据的写入、数据读出两个过程；内网与外网（或内网与专网）永不连接；内网和外网（或内网与专网）在同一时刻最多只有一个同物理隔离设备建立非 TCP/IP 协议的数据连接。物理隔离的硬件原理

是利用单刀双掷开关使得内外处理单元分时存取共享存储设备完成数据交换，实现了在空气缝隙隔离情况下的数据交换。软件原理是通过应用层数据提取与安全审查达到杜绝基于协议层的攻击和增强应用层安全的效果。

物理隔离的数据传输机制是存储和转发。网络隔离则是在物理隔离的基础上，综合利用过滤、认证、日志等技术和专用硬件，保证两个网络在链路层断开的前提下实现数据安全传输和资源共享，实现一个综合的安全平台。

2．物理隔离技术的发展

物理隔离的发展先后经历了 5 代隔离技术。

（1）完全的隔离。此方法使得网络处于信息孤岛状态，做到了完全的物理隔离，需要至少两套网络和系统，更重要的是信息交流的不便和成本的提高，这样给维护和使用带来了极大的不便。

（2）硬件卡隔离。在客户端增加一块硬件卡，客户端硬盘或其他存储设备首先连接到该卡，然后再转接到主板上，通过该卡能控制客户端硬盘或其他存储设备。而在选择不同的硬盘时，同时选择了该卡上不同的网络接口，连接到不同的网络。但是，这种隔离产品有的仍然需要网络布线为双网线结构，产品存在着较大的安全隐患。

（3）数据转播隔离。利用转播系统分时复制文件的途径来实现隔离，切换时间非常久，甚至需要手工完成，不仅明显地减缓了访问速度，更不支持常见的网络应用，失去了网络存在的意义。

（4）空气开关隔离。它是通过使用单刀双掷开关，使得内外部网络分时访问临时缓存器来完成数据交换的，但在安全和性能上存在许多问题。

（5）安全通道隔离。此技术通过专用通信硬件和专有安全协议等安全机制，来实现内外部网络的隔离和数据交换，不仅解决了以前隔离技术存在的问题，并有效地把内外部网络隔离开来，而且高效地实现了内外网数据的安全交换，透明支持多种网络应用，成为当前隔离技术的发展方向。

3．已有物理隔离与数据自动交换技术

物理隔离一般是指通过网络与网络（包括电磁空间）分离来实现的网络隔离，它是网络隔离的一种形式，其目的是禁止网络之间的资源共享，防止一个网络的信息泄露到另一个网络上去。物理隔离就是必须严格从网络的物理层起就与其他系统彻底隔离开来。当然，能够实现基于第一层的物理隔离是再安全不过了，但是如果没有数据交换，就难以达到应用的效果和目的，安全也只是无本之木。

物理隔离技术自问世以来，经过实践的检验和应用，不断发展成熟，目前已经历了几个发展阶段，每个阶段都产生了一种具有代表性的产品或解决方案。目前，这些物理隔离产品和方案在国家机要部门内部都有应用，但由于这些产品和方案存在一些缺陷与不足，还需要进一步的深入研究。以下是已有产品的物理隔离技术的几种类型。

（1）双机双网技术。是指配置两台计算机、分别联接内外两个网络。它通过移动存

储设备（如移动硬盘）交换数据。这种方式存在着一些缺点，如导致投资成本的增加、占用较大空间等。另外，双机的使用会带来很多不便，网络设置复杂、维护难度也较大，一旦出现问题，会使对效率要求相当高的部门受到很大影响。

（2）双硬盘隔离卡技术。是指在原有机器上增加一块硬盘和一个隔离卡来实现物理隔离，两块硬盘分别对应内外网，用户启动外网时关闭内网硬盘，启动内网时关闭外网硬盘。此种隔离方式需要用户在原有基础上再多加一块硬盘，对于一些配置比较高、原有硬盘比较大的机器而言，造成了无谓的成本浪费，而且频繁地加电和断电容易对原有硬盘造成损坏。由于双硬盘隔离卡存在很多缺点，它只能作为物理隔离技术发展过程中的替代产品存在。

（3）单硬盘隔离卡（客户端的物理隔离）技术。单硬盘隔离卡是目前国内采用的比较多的客户端物理隔离产品，国外也有类似的隔离技术产品。其实现原理是将原计算机（客户端）的单个硬盘从物理层上分割为公共和安全两个分区，安装两套操作系统，实现内外网的安全隔离。虽然单硬盘隔离卡有严密的硬盘数据保护功能，并有较强的可扩展功能，如可实现数据安全传输功能等，但是也很难界定数据是否安全。最大的缺陷是不能同时访问内外两个网络，访问不同的网络需要重新开机和启动，特别是对于经常访问内外两个网络的用户，需要频繁地在内外两个网络之间进行切换的应用很不方便。

（4）集线器级的物理隔离。集线器级的物理隔离产品需要与客户端的物理隔离产品结合起来应用，可以在客户端的内外双网的布线上使用一条网络线来通过远端切换器连接内外双网，实现一台工作站连接内外两个网络的目的，并在网络布线上避免了客户端计算机要用两条网络线连接网络。

（5）服务器端的物理隔离技术。服务器端的物理隔离产品是一种崭新的高级隔离产品，它通过复杂的软硬件技术实现了在服务器端的数据过滤和传输任务，其技术关键还是在同一时刻内外网络没有物理上的数据连通，但又快速分时地处理并传递数据。

综合考虑安全性能、资源占用、费用、维护和管理等因素，单机双网是目前应用较广泛的隔离方法。用户可以根据自己的需要使用热启动在不同的网络环境（内网或外网）中自由切换，操作时还不是十分方便。另外，双硬盘隔离卡、单硬盘隔离卡并没有满足有关不小于 5m 的规定。

网络的物理隔离是很多网络设计者都不愿意的选择，网络上要承载专用的业务，其安全性一定要得到保障。然而，网络的建设就是为了互通的，没有数据的共享，网络的作用也缩水了不少，因此网络隔离与数据交换是一对矛盾，如何解决好网络的安全，同时又方便地实现数据交换是网络规划设计中的重要内容。

以下的组图可以给我们一个清晰的概念，在数据交换时网络隔离是如何实现的。

如图 4-104 所示，外网是安全性不高的因特网，内网是安全性很高的内部网络。正常情况下，隔离设备的外部主机和外网相连，隔离设备的内部主机和内网相连，外网和

内网是完全断开的。隔离设备是一个独立的固态存储介质和一个单纯的调度控制电路。

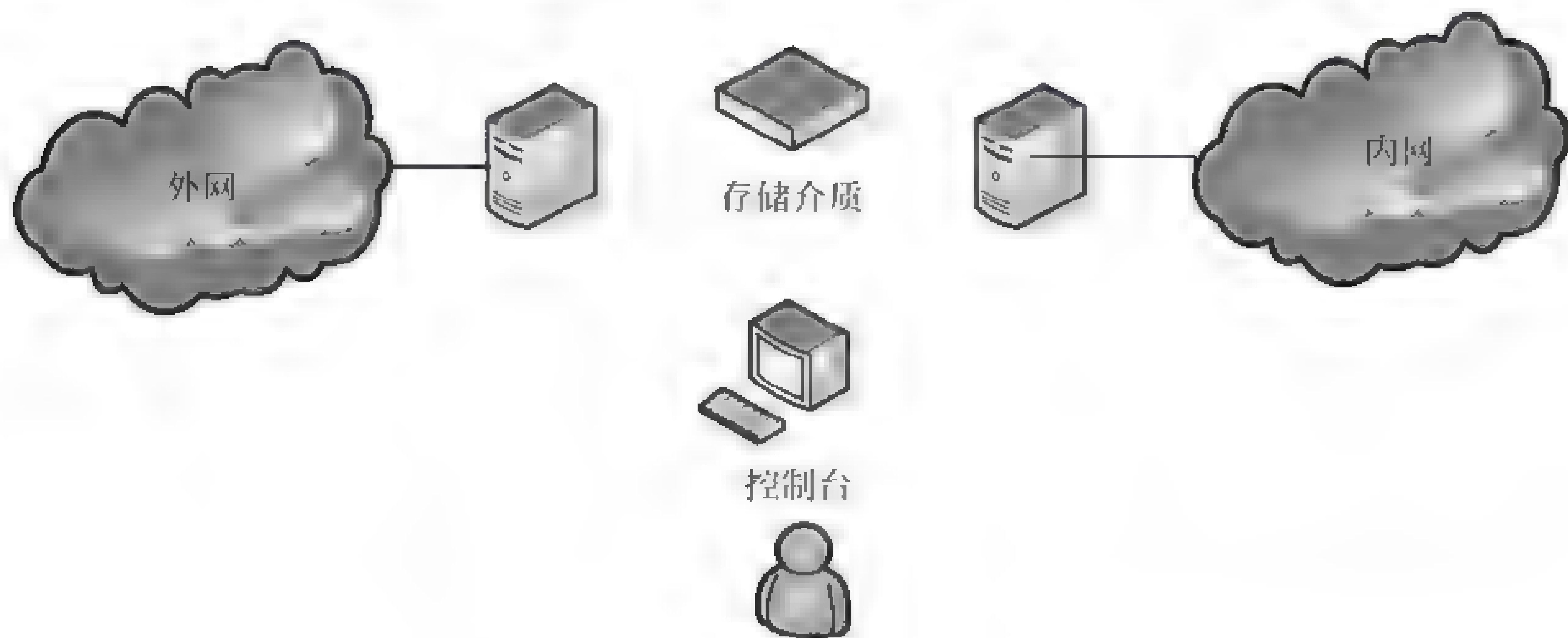


图 4-104　无数据交换的网络断开图

当外网需要有数据送达内网时，以电子邮件为例，外部主机先接收数据，并发起对固态存储介质的非 TCP/IP 协议的数据连接，外部主机将所有的协议剥离，将原始数据写入固态存储介质。如图 4-105 所示。根据不同的应用，可能有必要对数据进行完整性和安全性检查，如防病毒和恶意代码等。

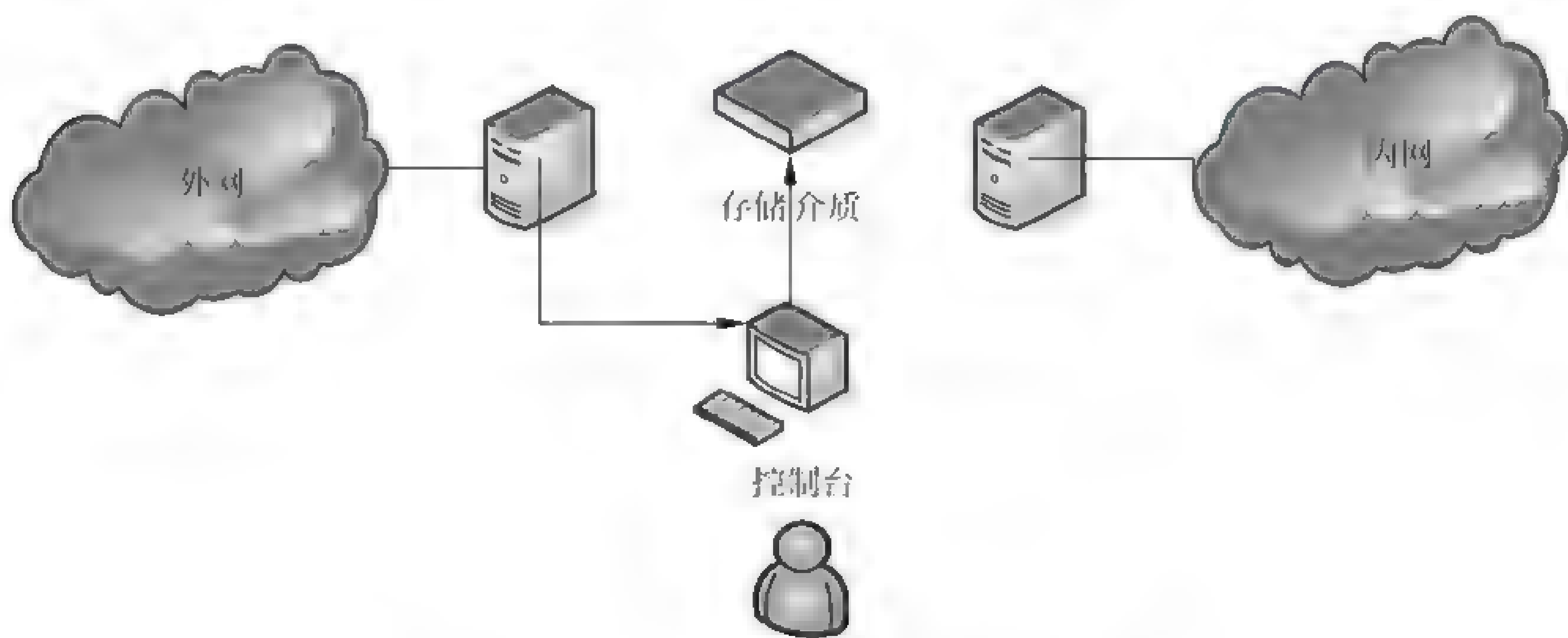


图 4-105　外部主机与固态存储介质交换数据示意图

一旦数据全部写入存储介质，立即中断与外部主机的连接。恢复到图 4-102 的状态，转而发起对内部主机的非 TCP/IP 协议的数据连接。固态存储介质将数据发送给内部主机。内部主机收到数据后，立即进行 TCP/IP 的封装和应用协议的封装，并发送给内网。如图 4-106 所示。这个时候内网电子邮件系统就收到了外网的电子邮件系统通过网络隔离设备转发的电子邮件。

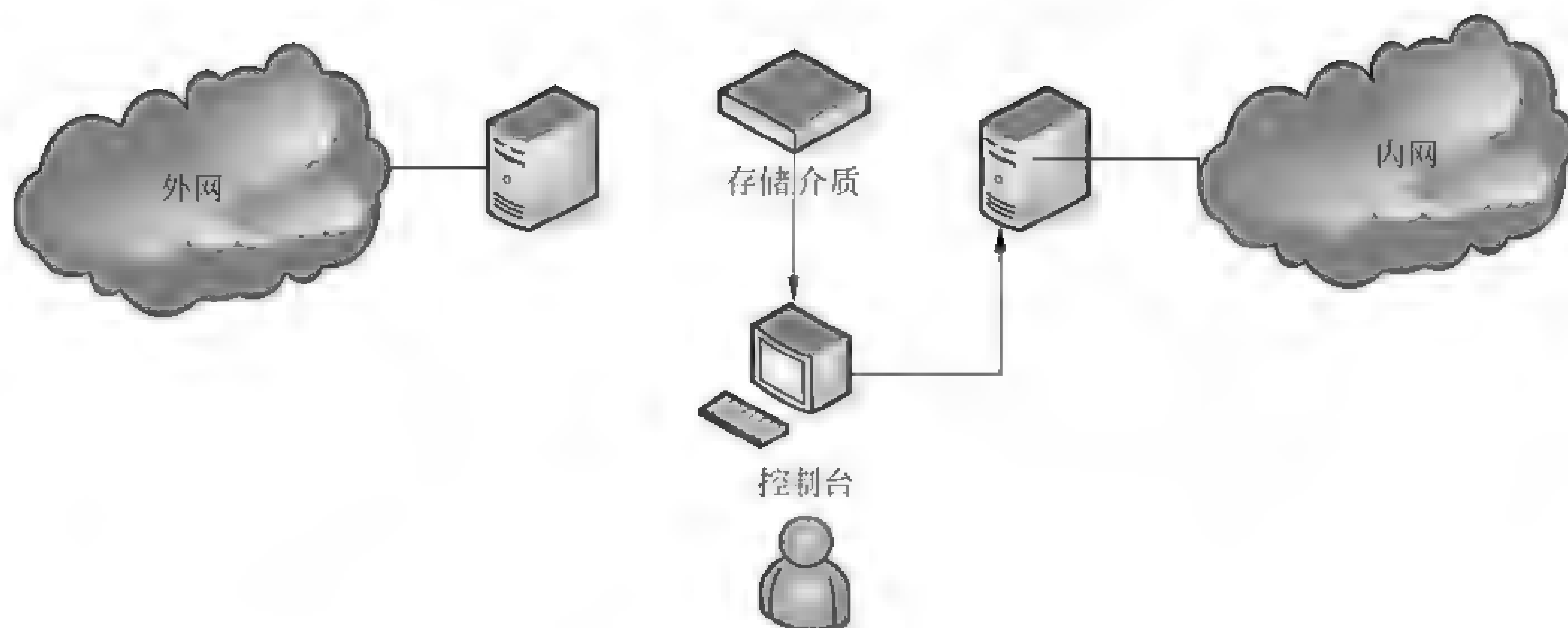


图 4-106 固态存储介质与内部主机数据交换示意图

在控制台收到完成数据交换任务的信号之后，立即切断与内部主机的直接连接，恢复到网络断开的初始状态。

如果这时内网有电子邮件要发出，内部主机先接收内部的数据，并建立与固态存储介质之间的非 TCP/IP 协议的数据连接。内部主机剥离所有的 TCP/IP 协议和应用协议，得到原始的数据，将数据写入存储介质。对其进行防病毒处理、防泄密和防恶意代码检查。然后中断与内部主机的直接连接。

一旦数据全部写入存储介质，立即中断与内部主机的连接。恢复到图 4-102 的状态，转而发起对外部主机的非 TCP/IP 协议的数据连接。网络隔离将存储介质内的数据发送给外部主机。外部主机收到数据后，立即进行 TCP/IP 的封装和应用协议的封装，并发送给外网。控制台收到处理完毕的信息后，立即中断隔离设备与外网的连接，恢复到完全隔离状态。

每一次数据交换，隔离设备都经历了数据的接收、存储和转发三个过程。由于这些规则都是在内存和内核里完成的，因此速度上有保证，可以达到 100%的总线处理能力。

4. 网闸和 GAP 技术

网络物理隔离的一个特征，就是内网与外网永不连接。内部主机和外部主机在同一时间最多只有一个同固态存储介质建立非 TCP/IP 协议的数据连接。网络隔离的好处是明显的，即使外网在最坏的情况下，内网也不会有任何破坏，修复外网系统也非常容易。以上这种基于两个单边主机（内部主机和外部主机）之间数据交换的网络隔离技术，被称作网闸。

网闸的设计原理是基于“代理+摆渡”的概念。如果把逻辑隔离比作在河上架桥，网闸可以比作在河上设摆渡船，摆渡船不直接连接两岸，安全性当然要比桥好，即使是攻击，也不可能一下就进入，并且在船上总要受到管理者的各种控制。协议隔离的原理

则是禁止采用“集装箱运输”，即通信协议落地，用专用协议、单向通道技术和存储等方式阻断业务的连接，用代理方式支持上层业务。网闸的功能有代理，这个代理不只是协议代理，还有数据的“拆卸”，把数据还原成原始的部分，拆除各种通信协议添加的“包头包尾”。很多攻击是通过对数据的拆装来隐藏自己的，没有了这些“通信管理”，攻击的入侵就很难进入。网闸的原理如图 4-107 所示。

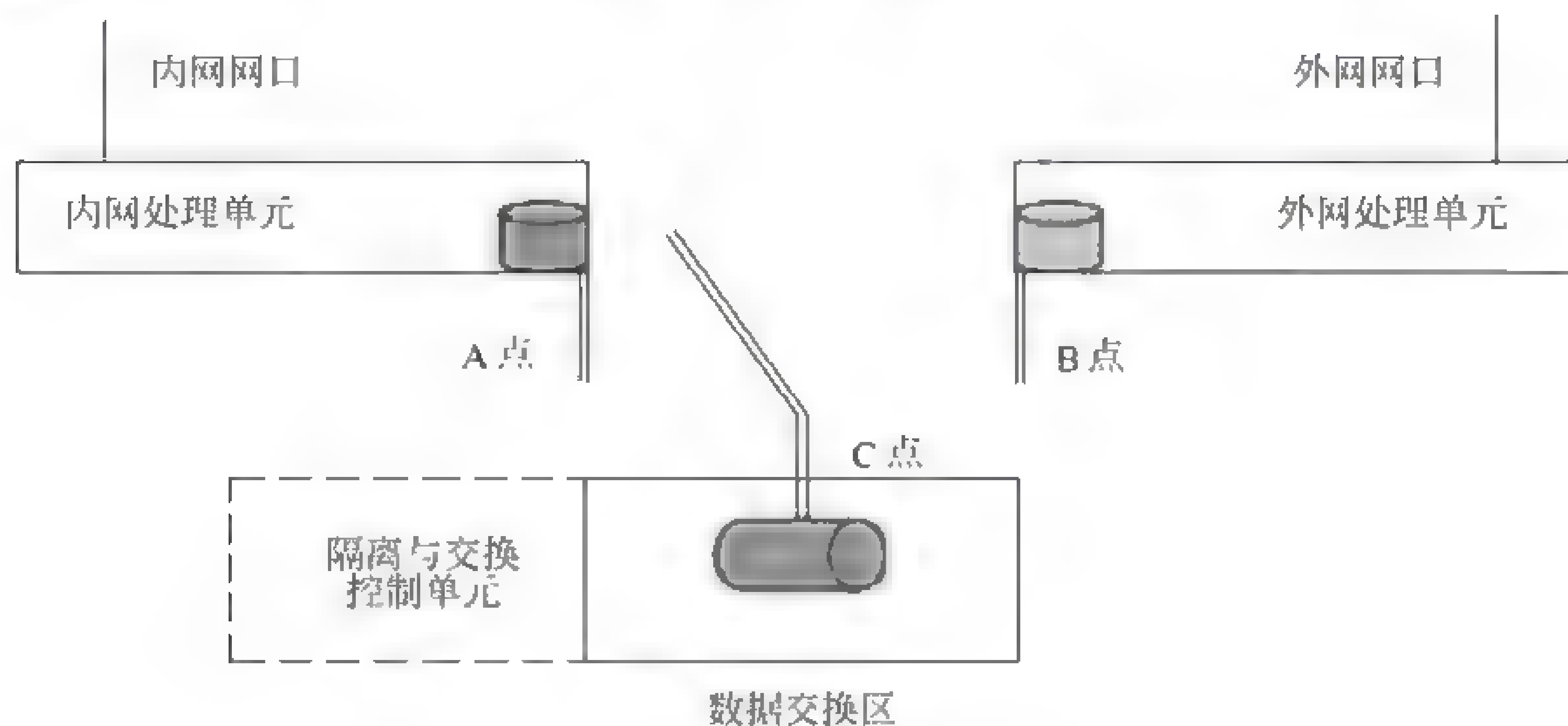


图 4-107　网闸的原理

网闸是很多安全网络隔离的选择，但网闸代理业务的方式不同，协议隔离的概念不断变化，所以在选择网闸时要注意网闸的具体实现方式。

目前网闸采用的主要技术是 GAP 技术。它是一种由带有多种控制功能的专用硬件在电路上切断网络之间的链路层连接，同时能够在网络间进行安全适度的应用数据交换的网络安全设备。GAP 又称为 AirGap，是指由空气形成的用于隔离的缝隙。GAP 技术是在 1997 年左右，最早由以色列的 Whale、Spearllead 等公司研制开发。2000 年，此类产品开始在国内出现。

目前主要有三类 GAP 技术：实时开关（RealTime Switch）、单向连接（One-Way link）和网络开关（Network Switch）。

实时开关的原理是使用硬件连接两个网络，两个网络之间通过硬件开关来保证不同时连通。通过开关的快速切换，并剥去 TCP 报头，通过不可路由的数据转存池来实现数据转发。

单向传输是指数据只能从一个网络单向向另外一个网络摆渡数据，两个网络是完全断开的。单向连接实际上通过硬件实现一条“只读”的单向传输通道来保证安全隔离。

网络切换器即将一台机器虚拟成两套设备，通过开关来确保两套设备不连通，同一时刻最多只有一个虚拟机是激活的。这种隔离技术虽确保了安全性，但实时性较差，不过成本较低。

4.9 公钥基础结构

4.9.1 公钥密码

4.9.1.1 公钥密码的思想

PKI 所依赖的核心思想是公钥密码。传统密码及装置中，转轮机器和 DES 是密码学发展的重要标志，但是它们都是基于替换和置换这些初等方法。公钥密码学与其前的密码学完全不同。公钥算法是基于数学函数而不是基于替换和置换，此外，与只使用一个密钥的对称传统密码不同，公钥密码学是非对称的，它依赖于一个公开密钥和一个与之在数学上相关但不相同的私钥，且仅根据密码算法和公开密钥来确定私钥在计算上是不可行的。公开钥用于加密和签名认证，私钥则对应地用于解密和签名。

使用两个密钥在消息的秘密性、密钥分配和认证领域有着重要意义。公钥密码可以有效解决传统密码中最困难的两个问题：密钥分配问题和数字签名问题。

一是密钥分配问题，用传统密码进行密钥分配要求通信双方或者已经共享一个密钥，而该密钥已通过某种方法分配给通信双方；或者利用密钥分配中心。公钥密码的发明人之一 Whitfield Diffie 认为，第二个要求有悖于密码学的精髓，即应在通信过程中完全保持秘密性。“如果必须要求用户与 KDC 共享他们的密钥，这些密钥可能因为盗窃或索取而被泄密，那么设计不可破的密码体制究竟还有什么意义呢？”

第二个问题是数字签名问题，即将密码学用于电子消息和文件的签名，并能确保数字签名是出自某人，并且各方对此均无异议。

4.9.1.2 公钥加密算法

1976 年，Diffie 和 Hellman 针对上述两个问题公开提出公钥密码算法。公钥密码算法依赖于一个加密密钥和一个与之相关但不同的解密密钥，这些算法具有这样的特点，即仅根据密码算法和加密密钥来确定解密密钥在计算上是不可行的。公钥加密的主要步骤如下。

（1）网络中的每个终端系统生成一对密钥，用来加密和解密消息。

（2）每个终端系统通过将其加密密钥存于公开的寄存器或文件中，公布其加密密钥，这个密钥称为公钥；而其解密密钥则是秘密的。

（3）若 A 要发消息给 B，则 A 用 B 的公钥对消息加密。

（4）B 收到消息后，用其私钥对消息解密。由于只有 B 知道其私钥，所以其他的接收者均不能解出消息。

到目前为止，被广泛接受的公钥密码系统主要是大整数因子分解 IFP 困难性的 RSA

系统和基于椭圆曲线离散对数 ECDLP 的计算困难性的 ECC 系统。

MIT 的 Ron Rivest、Adi Shamir 和 Len Adleman 于 1977 年提出并于 1978 年首次发表的算法[RIVE78]，可以说是最早提出的公钥算法之一。Rivest Shamir Adleman（RSA）算法自其诞生之日起就一直是最为重要的公钥算法。

RSA 体制是一种分组密码，其明文和密文均是 0～n-1 之间的整数。RSA 系统的安全性主要是基于大整数因子分解的困难性，而大整数因子分解问题是数学上的著名难题，至今没有有效的方法予以解决，因此可以确保 RSA 算法的安全性。RSA 算法的明文以分组为单位进行加密，每个分组的二进制值均小于 n。也就是说，分组的大小必须小于或等于 $\log_2$（n）位。在实际应用中，分组的大小是 k 位，其中 $2^k < n \le 2^{k+1}$。对明文分组 M 和密文分组 C，加密和解密过程如下。

加密过程：$C = M^e \mod n$

解密过程：$M = C^d \mod n = (M^e)^d \mod n = M^{ed} \mod n$

其中，收发双方均已知 n，发方已知 e，只有收方已知 d，公钥为 KU＝{e，n}，私钥为 KR＝{d，n}。算法的参数满足下列条件：

素数 p 和 q 为素数	（保密，由用户选定）
$n = pq$	（公开，由计算得出）
e 满足 $\gcd(\phi(n), e) = 1$；$1 < e < \phi(n)$	（公开，由用户选定）
$d \equiv e^{-1} \mod \phi(n)$	（保密，由计算得出）

ECC 系统的安全性主要依赖于椭圆曲线离散对数的计算困难性。自 1985 年，Neal Koblitz 和 Victor Miller 提出 ECC 算法以来，ECC 密码系统的协议和标准被多家著名国际标准组织所接受。建立在椭圆曲线离散对数问题上的加密方法则称为椭圆曲线加密方法，简称 ECC 方法，它较通常的离散对数问题更为困难，因此可以确保 ECC 系统的安全性。ECC 算法的安全性来源于它的破解需要指数级的运算；而 RSA 的破解只需要次指数级的运算。较之于 RSA，基于离散对数问题的 ECC 系统由于其基础域的表示非常丰富，因此，在此基础上可对其表示进行优化。而 RSA 及离散对数问题的素数选择必须满足“安全性原则”，因此受到了更多的限制。通过比较破解 ECC 和破解 RSA 的年数可以知道，ECC 要想得到与 RSA 相当的安全性，只需要短得多的密钥。例如，192 位模长的 ECC 的安全性与 1600 位模长的 RSA 的安全性相当。显然，更小的密钥将可以带来更小的系统参数、更小的公钥证书，耗用更小的带宽、速度更快、能耗更低、处理器更小。在广泛的研究和密码经验的基础上，诸多产业领先者都已经将椭圆曲线密码系统作为一种成熟技术应用于产业领域。

4.9.1.3　数字签名算法

数字签名是利用一套规则和一个参数集对数据计算所得的结果，用此结果能够确认签名者的身份和数据的完整性，这里的数据计算通常是密码变换。

简单地说，数字签名就是附加在数据单元上的一些数据，或是对数据单元所作的密码变换。这种数据或变换允许数据单元的接收者用以确认数据单元的来源和数据单元的完整性并保护数据，防止被他人进行伪造。基于公钥密码体制和私钥密码体制都可以获得数字签名，目前主要是基于公钥密码体制的数字签名，包括普通数字签名和特殊数字签名。普通数字签名算法有 RSA、ElGamal、Fiat-Shamir、Guillou- Quisquarter、Schnorr、Ong-Schnorr-Shamir 数字签名算法、DSA、椭圆曲线数字签名算法和有限自动机数字签名算法等。特殊数字签名有盲签名、代理签名、群签名、不可否认签名、公平盲签名、门限签名和具有消息恢复功能的签名等，它与具体应用环境密切相关。

数字签名（digital signature）技术是不对称加密算法的典型应用。数字签名的应用过程是，数据源发送方使用自己的私钥对数据校验和或其他与数据内容有关的变量进行加密处理，完成对数据的合法“签名”，数据接收方则利用对方的公钥来解读收到的“数字签名”，并将解读结果用于对数据完整性的检验，以确认签名的合法性。数字签名技术是在网络系统虚拟环境中确认身份的重要技术，完全可以代替现实过程中的“亲笔签字”，在技术和法律上有保证。数字签名主要的功能是：保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生。

数字签名技术是将摘要信息用发送者的私钥加密，与原文一起传送给接收者。接收者只有用发送的公钥才能解密被加密的摘要信息，然后用 hash 函数对收到的原文产生一个摘要信息，与解密的摘要信息对比。如果相同，则说明收到的信息是完整的，在传输过程中没有被修改，否则说明信息被修改过，因此数字签名能够验证信息的完整性。

美国国家标准与技术研究所（NIST）发布的联邦信息处理标准 FIPS PUB186，称为数字签名标准 DSS。DSS 利用安全 hash 算法 SHA 和公钥技术，给出了数字签名算法（DSA）。DSS 使用的是只提供数字签名功能的算法。与 RSA 不同，DSS 是一种公钥方法，但不能用于加密或密钥分配。在 RSA 方法中，hash 函数的输入是要签名的消息，输出是定长的 hash 码，用发方的私钥对该 hash 码加密形成签名，然后发送消息及其签名。收方用发方的公钥对签名解密，如果计算出的 hash 码与解密出的结果相同，则认为签名是有效的。因为只有发方拥有私钥，因此只有发方能够产生有效的签名。DSA 则是建立在求离散对数的困难性之上的。

4.9.2 PKI 组成

4.9.2.1 PKI 的概念

公钥基础设施（Public Key Infrastructure，PKI）是一个采用公钥概念和技术来提供安全服务的具有普适性的安全基础设施，是目前网络安全建设的基础与核心。PKI 由公开密钥密码技术、数字证书、证书发放机构和关于公开密钥的安全策略等基本成分共同组成的。

PKI 采用证书进行公钥管理，通过第三方的可信任机构（认证中心，即 CA），把用户的公钥和用户的其他标识信息捆绑在一起，其中包括用户名和电子邮件地址等信息，以在 Internet 上验证用户的身份。PKI 把公钥密码和对称密码结合起来，在 Internet 上实现密钥的自动管理，保证网上数据的安全传输。

因此，从大的方面来说，所有提供公钥加密和数字签名服务的系统，都可归结为 PKI 系统的一部分。PKI 的主要目的是通过自动管理密钥和证书，为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下方便地使用加密和数字签名技术，从而保证网上数据的机密性、完整性和有效性。数据的机密性是指数据在传输过程中不能被非授权者偷看；数据的完整性是指数据在传输过程中不能被非法篡改；数据的有效性是指数据不能被否认。

一个有效的 PKI 系统必须是安全的和透明的，用户在获得加密和数字签名服务时，不需要详细地了解 PKI 的内部运作机制。在一个典型、完整和有效的 PKI 系统中，除证书的创建和发布，特别是证书的撤消外，一个可用的 PKI 产品还必须提供相应的密钥管理服务，包括密钥的备份、恢复和更新等。没有一个好的密钥管理系统，将极大地影响一个 PKI 系统的规模、可伸缩性和在协同网络中的运行成本。在一个企业中，PKI 系统必须有能力为一个用户管理多对密钥和证书；能够提供安全策略编辑和管理工具，如密钥周期和密钥用途等。

PKI 作为一组在分布式计算系统中利用公钥技术和 X.509 证书所提供的安全服务，企业或组织可利用相关产品建立安全域，并在其中发布密钥和证书。在安全域内，PKI 管理加密密钥和证书的发布，并提供诸如密钥管理（包括密钥更新、密钥恢复和密钥委托等）、证书管理（包括证书产生和撤销等）和策略管理等。PKI 产品也允许一个组织通过证书级别或直接交叉认证等方式来同其他安全域建立信任关系。这些服务和信任关系不能局限于独立的网络之内，而应建立在网络之间和 Internet 之上，为电子商务和网络通信提供安全保障，所以具有互操作性的结构化和标准化技术成为 PKI 的核心。

PKI 在实际应用上是一套软硬件系统和安全策略的集合，它提供了一整套安全机制，使用户在不知道对方身份或分布地很广的情况下，以证书为基础，通过一系列的信任关系进行通信和电子商务交易。

PKI 体系结构如图 4-108 所示。

4.9.2.2　典型的 PKI 系统组成

一个典型的 PKI 系统如图 4-109 所示，其中包括 PKI 策略及软硬件系统、证书机构、注册机构、证书发布系统和 PKI 应用等。

（1）PKI 策略及软硬件系统。PKI 安全策略建立和定义了一个组织信息安全方面的指导方针，同时也定义了密码系统使用的处理方法和原则。它包括一个组织怎样处理密

钥和有价值的信息，根据风险的级别定义安全控制的级别。一般情况下，PKI 中有两种类型的策略：一是证书策略，用于管理证书的使用，如可以确认某一 CA 是在 Internet 上的公有 CA，还是某一企业内部的私有 CA；另外一种就是 CPS（Certificate Practice Statement）。一些由商业证书发放机构（CCA）或者可信的第三方操作的 PKI 系统需要 CPS，它实际上是一些操作过程的详细文档，描述了如何在实践中增强和支持安全策略，包括 CA 是如何建立和运作的，证书是如何发行、接收和废除的，密钥是如何产生、注册的，以及密钥是如何存储的，用户是如何得到它的等。

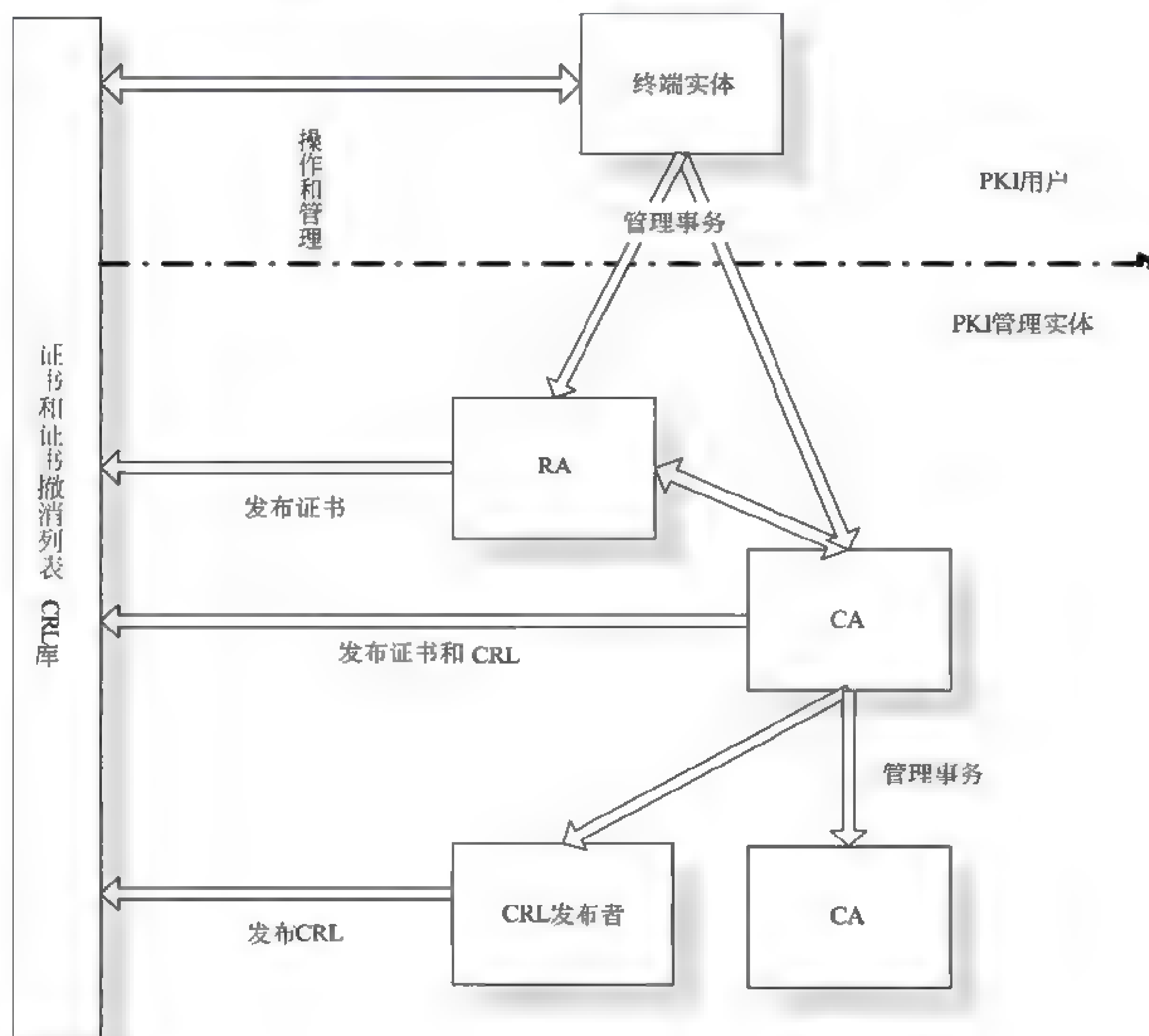


图 4-108　PKI 的体系结构

（2）证书机构。证书机构是 PKI 的信任基础，它管理公钥的整个生命周期，其作用包括发放证书、规定证书的有效期和通过发布证书废除列表（CRL）确保必要时可以废除证书。

（3）注册机构。注册机构提供用户和 CA 之间的一个接口，它获取并认证用户的身份，向 CA 提出证书请求。它主要完成收集用户信息和确认用户身份的功能。这里的用

户是指将要向认证中心申请数字证书的客户，可以是个人，也可以是集团或团体、某政府机构等。注册管理一般由一个独立的注册机构来承担。它接受用户的注册申请，审查用户的申请资格，并决定是否同意 CA 给其签发数字证书。注册机构并不给用户签发证书，而只是对用户进行资格审查。因此，RA 可以设置在直接面对客户的业务部门，如银行的营业部、机构认识部门等。当然，对于一个规模较小的 PKI 应用系统来说，可把注册管理的职能由认证中心来完成，而不设立独立运行的 RA。但这并不是取消了 PKI 的注册功能，而只是将其作为 CA 的一项功能而已。PKI 国际标准推荐由一个独立的 RA 来完成注册管理的任务，可以增强应用系统的安全。

（4）证书发布系统。证书发布系统负责证书的发放，如可以通过用户自己或是通过目录服务。目录服务器可以是一个组织中现存的，也可以是 PKI 方案中提供的。

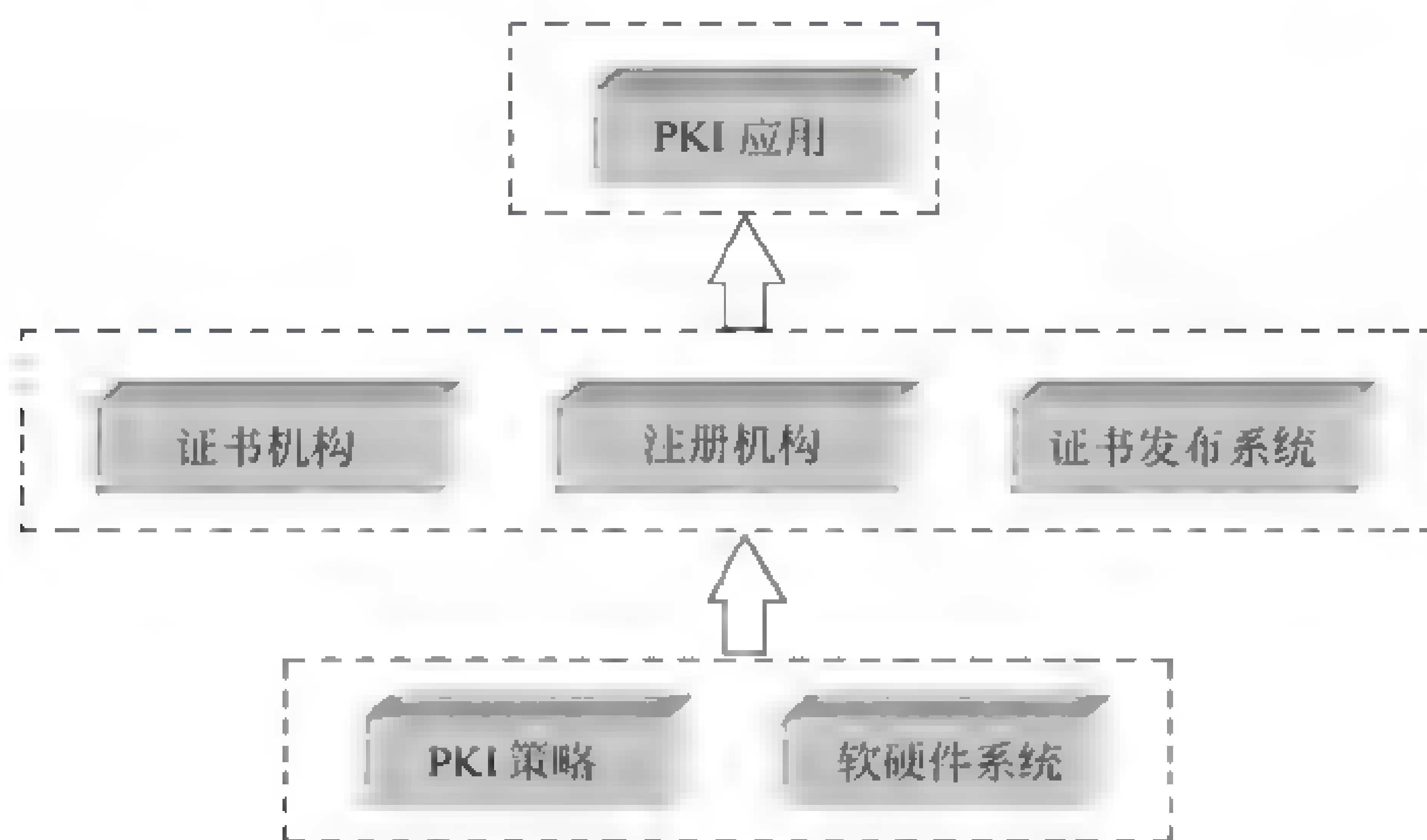


图 4-109　PKI 组成框图

4.9.3　证书认证机构

4.9.3.1　X.509 证书和 CRL

X.509 证书是由国际电信联盟（ITU-T）为了提供公用网络用户目录信息服务，于 1988 年制定的数字证书标准。其中，X.500 和 X.509 是安全认证系统的核心，X.500 定义了一种区别命名规则，以命名来确保用户名称的唯一性，X.509 则为 X.500 用户名称提供了通信实体鉴别机制，并规定了督促检查体鉴别过程中广泛适用的证书语法和数据接口，X.509 称之为证书。

用户公钥证书是 X.509 的核心，证书由某个可信的证书发放机构建立，并由 CA 或用户自己将其放入目录中，以供其他用户方便地访问。X.509 证书由用户公共密钥与用

户标识符组成，此外还包括版本号、证书序列号、CA 标识符和签发算法标识等，具体格式如下所述。



其中各参数的含义如下。

- 证书版本号（Version）：指明 X.509 证书的格式版本，现在的值可以为 0，1，2，也为将来的版本进行了预定义。
- 证书序列号（SerialNumber）：序列号指定由 CA 分配给证书的唯一的数字型标识符。当证书被取消时，实际上是将此证书的序列号放入由 CA 签发的 CRL 中，这也是序列号唯一的原因。
- 签名算法标识符（Signature）：用来指定由 CA 签发证书时所使用的签名算法。算法标识符用来指定 CA 签发证书时所使用的公开密钥算法和 hash 算法，须向国际知名标准组织（如 ISO）注册。
- 签发机构名（Issuer）：此域用来标识签发证书的 CA 的 X.500 DN 名字。包括国家、省市、地区、组织机构、单位部门和通用名。
- 有效期（Validity）：指定证书的有效期，包括证书开始生效的日期和时间以及失效的日期和时间。每次使用证书时，需要检查证书是否在有效期内。
- 证书用户名（Subject）：指定证书持有者的 X.500 唯一名字。包括国家、省市、地区、组织机构、单位部门和通用名，还可包含 E-mail 地址等个人信息等。
- 证书持有者公开密钥信息（SubjectPublicKeyInfo）：包含证书持有者的公开密钥的值和公开密钥使用的算法标识符两个重要信息。此标识符包含公开密钥算法和

hash 算法。

- 签发者唯一标识符（Issuer Unique Identifier）：在第 2 版加入证书定义中。此域用在当同一个 X.500 名字用于多个认证机构时，用一位字符串来唯一标识签发者的 X.500 名字。可选。
- 证书持有者唯一标识符（Subject Unique Identifier）：在第 2 版的标准中加入 X.509 证书定义。此域用在当同一个 X.500 名字用于多个证书持有者时，用一位字符串来唯一标识证书持有者的 X.500 名字。可选。
- 签名值（Issuer's Signature）：证书签发机构对证书上述内容的签名值。

为了适应 PKI 技术的发展，IETF 也必须制定在 Internet 上使用 X.509 和 CRL 的标准。PKIX 工作组就提供了一个 Internet 草案 Part I： X.509 Certificate and CRL Profile（详细内容可见 ftp：//ftp.ietf.org/internet-drafts/draft-ietf-pkix-ipki-part1-11.txt），用于定义在 Internet PKI 中使用 X.509 和 CRL 的方法和规范。该草案把 X.509 作为标准，并对各标准项和扩展做了说明，基本接收了 X.509 作为 Internet 中的证书标准，但也定义了被 PKI 应用的 X.509 V3 和 CRL V2 标准格式的设置，这些设置包含了 PKIX 工作组对 X.509 所做的一些新的扩展。

X.509 目前有三个版本：V1、V2 和 V3，其中，V3 是在 V2 的基础上加上扩展项后的版本，这些扩展包括由 ISO 文档（X.509-AM）定义的标准扩展，也包括由其他组织或团体定义或注册的扩展项。X.509 由 ITU-T X.509（前身为 CCITT X.509）或 ISO/IEC 9594-8 定义，最早以 X.500 目录建议的一部分发表于 1988 年，并作为 V1 版本的证书格式。X.500 于 1993 年进行了修改，并在 V1 基础上增加了两个额外的域，用于支持目录存取控制，从而产生了 V2 版本。

为了适应新的需求，ISO/IEC 和 ANSI X9 发展了 X.509 V3 版本证书格式，该版本证书通过增加标准扩展项对 V1 和 V2 证书进行了扩展。另外，根据实际需要，各个组织或团体也可以增加自己的私有扩展。X.509 V3 证书是在 V2 的基础上以标准形式或普通形式增加的扩展项，以使证书能够附带额外信息。标准扩展是指由 X.509 V3 版本定义的对 V2 版本增加的具有广泛应用前景的扩展项，任何人都可以向一些权威机构如 ISO，来注册一些其他扩展，如果这些扩展项应用广泛，也许以后会成为标准扩展项。

证书废除列表（Certificate Revocation Lists，CRL，又称证书黑名单）为应用程序和其他系统提供了一种检验证书有效性的方式。任何一个证书废除以后，证书机构会通过发布 CRL 的方式来通知各个相关方。目前，同 X.509 V3 证书对应的 CRL 为 X.509 V2 CRL，其所包含的内容格式如下。

- CRL 的版本号：0 表示 X.509 V1 标准；1 表示 X.509 V2 标准。目前常用的是同 X.509 V3 证书对应的 CRL V2 版本。
- 签名算法：包含算法标识和算法参数，用于指定证书签发机构用来对 CRL 内容进行签名的算法。

- 证书签发机构名：签发机构的 DN 名，由国家、省市、地区、组织机构、单位部门和通用名等组成。
- 此次签发时间：此次 CRL 签发时间，遵循 ITU-T X.509 V2 标准的 CA 在 2049 年之前把这个域编码为 UTCTime 类型，在 2050 年或 2050 年之后把这个域编码为 GeneralizedTime 类型。
- 下次签发时间：下次 CRL 签发时间，遵循 ITU-T X.509 V2 标准的 CA 在 2049 年之前把这个域编码为 UTCTime 类型，在 2050 年或 2050 年之后把这个域编码为 GeneralizedTime 类型。
- 用户公钥信息，其中包括废除的证书序列号和证书废除时间。废除的证书序列号是指要废除的由同一个 CA 签发的证书的一个唯一标识号，同一机构签发的证书不会有相同的序列号。
- 签名算法：对 CRL 内容进行签名的签名算法。
- 签名值：证书签发机构对 CRL 内容的签名值。

另外，CRL 中还包含扩展域和条目扩展域。CRL 扩展域用于提供与 CRL 有关的额外信息部分，允许团体和组织定义私有的 CRL 扩展域来传送他们独有的信息；CRL 条目扩展域则提供与 CRL 条目有关的额外信息部分，允许团体和组织定义私有的 CRL 条目扩展域来传送他们独有的信息。

数字证书作为一种电子数据格式，可以直接从网上下载，也可以通过其他方式。

可使用 IC 卡存放用户证书。即把用户的数字证书写到 IC 卡中，供用户随身携带。这样用户在所有能够读 IC 卡证书的电子商务终端上都可以享受安全电子商务服务。

用户证书也可直接存放在磁盘或自己的终端上。用户将从 CA 申请来的证书下载或复制到磁盘或自己的 PC 或智能终端上，当用户使用自己的终端享受电子商务服务时，直接从终端读入即可。

另外，CRL 一般通过网上下载的方式存储在用户端。

4.9.3.2 CA 框架模型

CA 用于创建和发布证书，它通常为一个称为安全域（security domain）的有限群体发放证书。创建证书时，CA 系统首先获取用户的请求信息，其中包括用户公钥（公钥一般由用户端产生，如电子邮件程序或浏览器等），CA 将根据用户的请求信息产生证书，并用自己的私钥对证书进行签名。其他用户、应用程序或实体将使用 CA 的公钥对证书进行验证。如果一个 CA 系统是可信的，则验证证书的用户可以确信，他所验证的证书中的公钥属于证书所代表的那个实体。

CA 还负责维护和发布 CRL。当一个证书，特别是其中的公钥因为其他原因无效时（不是因为到期），CRL 提供了一种通知用户和其他应用的中心管理方式。CA 系统生成 CRL 以后，要么是放到 LDAP 服务器中供用户查询或下载，要么是放置在 Web 服务器

的合适位置，以页面超链接的方式供用户直接查询或下载。

一个典型的 CA 系统包括安全服务器、注册机构、CA 服务器、LDAP 目录服务器和数据库服务器等。如图 4-110 所示。

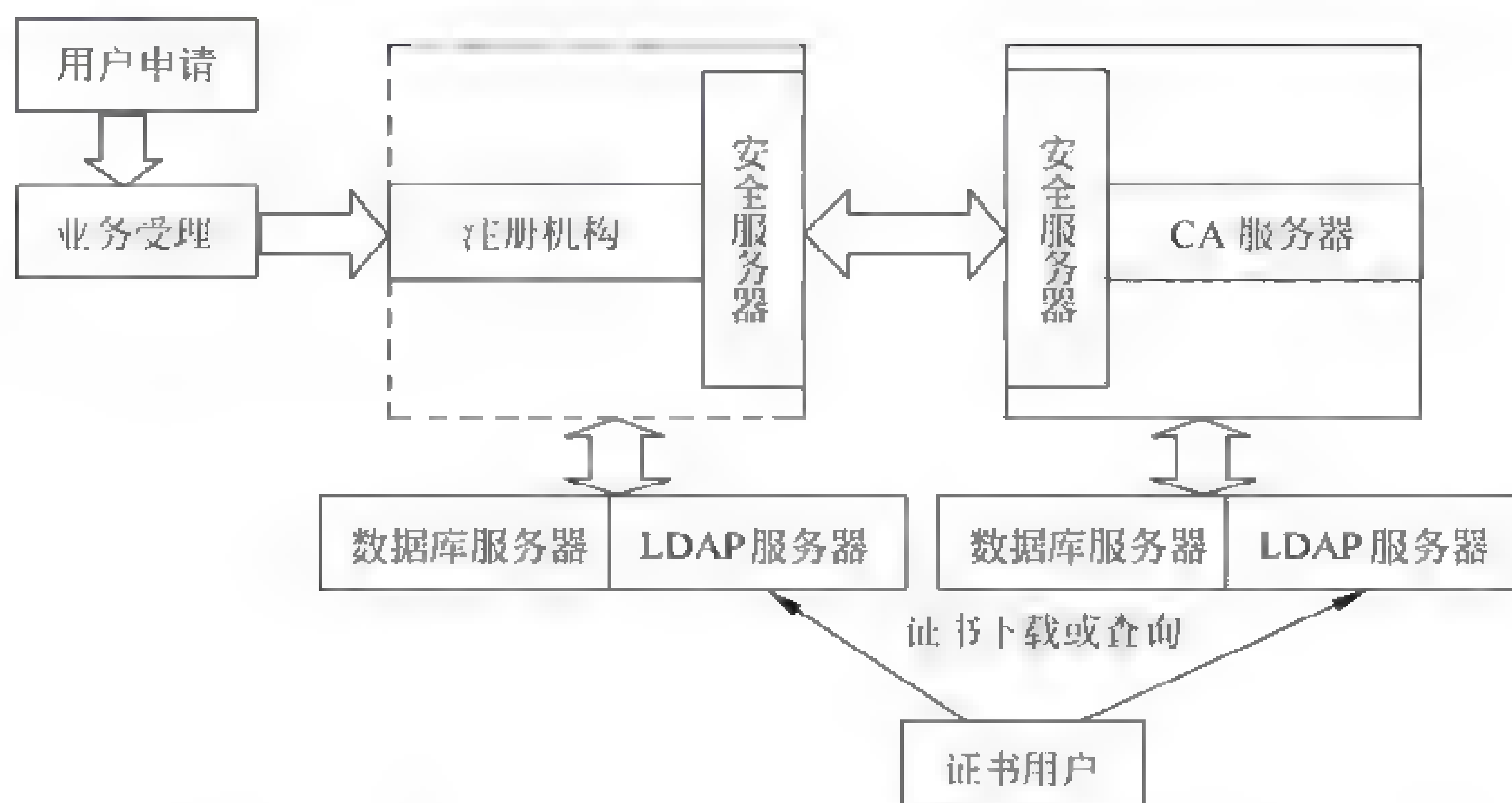


图 4-110　典型 CA 框架模型

（1）安全服务器。安全服务器面向普通用户，用于提供证书申请、浏览、证书撤销列表以及证书下载等安全服务。安全服务器与用户的通信采取安全信道方式（如 SSL 的方式，不需要对用户进行身份认证）。用户首先得到安全服务器的证书（该证书由 CA 颁发），然后用户与服务器之间的所有通信，包括用户填写的申请信息以及浏览器生成的公钥均以安全服务器的密钥进行加密传输，只有安全服务器利用自己的私钥解密才能得到明文，这样可以防止其他人通过窃听得到明文，从而保证了证书申请和传输过程中的信息安全性。

（2）CA 服务器。CA 服务器使整个证书机构的核心，负责证书的签发。CA 首先产生自身的私钥和公钥（密钥长度至少为 1024 位），然后生成数字证书，并且将数字证书传输给安全服务器。CA 还负责为操作员、安全服务器以及注册机构服务器生成数字证书。安全服务器的数字证书和私钥也需要传输给安全服务器。CA 服务器是整个结构中最为重要的部分，存有 CA 的私钥以及发行证书的脚本文件，出于安全的考虑，应将 CA 服务器与其他服务器隔离，任何通信采用人工干预的方式，确保认证中心的安全。

（3）注册机构。登记中心服务器面向登记中心操作员，在 CA 体系结构中起承上启下的作用，一方面向 CA 转发安全服务器传输过来的证书申请请求，另一方面向 LDAP 服务器和安全服务器转发 CA 颁发的数字证书和证书撤消列表。

（4）LDAP 服务器。LDAP 服务器提供目录浏览服务，负责将注册机构服务器传输过来的用户信息以及数字证书加入到服务器上。这样，其他用户通过访问 LDAP 服务器就能够得到其他用户的数字证书。

（5）数据库服务器。数据库服务器是认证机构中的核心部分，用于认证机构中数据（如密钥和用户信息等）、日志及统计信息的存储和管理。实际的数据库系统应采用多种措施，如磁盘阵列、双机备份和多处理器等方式，以维护数据库系统的安全性、稳定性、可伸缩性和高性能。

4.9.3.3 证书的申请和撤消

证书的申请有两种方式：在线申请和离线申请。在线申请就是通过浏览器或其他应用系统通过在线的方式来申请证书，这种方式一般用于申请普通用户证书或测试证书。离线方式一般通过人工的方式直接到证书机构证书受理点去办理证书申请手续，通过审核后获取证书，这种方式一般用于比较重要的场合，如服务器证书和商家证书等。下面讨论的主要是在线申请方式。

当证书申请时，用户使用浏览器通过 Internet 访问安全服务器，下载 CA 的数字证书（又叫做根证书），然后注册机构服务器对用户进行身份审核，认可后便批准用户的证书申请，然后操作员对证书申请表进行数字签名，并将申请及其签名一起提交给 CA 服务器。

CA 操作员获得注册机构服务器操作员签发的证书申请，发行证书或者拒绝发行证书，然后将证书通过硬复制的方式传输给注册机构服务器。注册机构服务器得到用户的证书以后，将用户的一些公开信息和证书放到 LDAP 服务器上提供目录浏览服务，并且通过电子邮件的方式通知用户从安全服务器上下载证书。用户根据邮件的提示到指定的网址下载自己的数字证书，而其他用户可以通过 LDAP 服务器获得他的公钥数字证书。

证书申请的步骤如下。

（1）用户申请。用户首先下载 CA 的证书，又叫根证书，然后在证书的申请过程中使用 SSL 安全方式与服务器建立连接，用户填写个人信息，浏览器生成私钥和公钥对，将私钥保存客户端特定文件中，并且要求用口令保护私钥，同时将公钥和个人信息提交给安全服务器。安全服务器将用户的申请信息传送给注册机构服务器。

（2）注册机构审核。用户与注册机构人员联系，证明自己的真实身份，或者请求代理人与注册机构联系。注册机构操作员利用自己的浏览器与注册机构服务器建立 SSL 安全通信，该服务器需要对操作员进行严格的身份认证，包括操作员的数字证书、IP 地址，为了进一步保证安全性，可以设置固定的访问时间。操作员首先查看目前系统中的申请人员，从列表中找出相应的用户，点击用户名，核对用户信息，并且可以进行适当的修改，如果操作员同意用户申请证书请求，必须对证书申请信息进行数字签名。操作员也有权利拒绝用户的申请。操作员与服务器之间的所有通信都采用加密和签名，具有安全性、抗否认性，保证了系统的安全性和有效性。

（3）CA 发行证书。注册机构通过硬复制的方式向 CA 传输用户的证书申请与操作员的数字签名，CA 操作员查看用户的详细信息，并且验证操作员的数字签名，如果签名验证通过，则同意用户的证书请求，颁发证书。然后 CA 将证书输出。如果 CA 操作

员发现签名不正确，则拒绝证书申请，CA 颁发的数字证书中包含关于用户及 CA 自身的各种信息，如能唯一标识用户的姓名及其他标识信息，如个人的 E-mail 地址；证书持有者的公钥。公钥用于为证书持有者加密敏感信息、签发个人证书的认证机构的名称、个人证书的序列号和个人证书的有效期（证书有效起止日期）等。

（4）注册机构证书转发。注册机构操作员从 CA 处得到新的证书，首先将证书输出到 LDAP 目录服务器以提供目录浏览服务，然后操作员向用户发送一封电子邮件，通知用户证书已经发行成功，并且把用户的证书序列号告诉用户，让用户到指定的网址去下载自己的数字证书。并且告诉用户如何使用安全服务器上的 LDAP 配置，让用户修改浏览器的客户端配置文件以便访问 LDAP 服务器，获得他人的数字证书。

（5）用户证书获取。用户使用证书申请时的浏览器到指定的网址，输入自己的证书序列号，服务器要求用户必须使用申请证书时的浏览器，因为浏览器需要用该证书相应的私钥去验证数字证书。只有保存了相应私钥的浏览器才能成功下载用户的数字证书。

这时用户打开浏览器的安全属性，就可以发现自己已经拥有了 CA 颁发的数字证书，可以利用该数字证书与其他人以及 Web 服务器（拥有相同 CA 颁发的证书）使用加密、数字签名进行安全通信。

认证中心还涉及到 CRL 的管理。用户向特定的操作员（仅负责 CRL 的管理）发一份加密签名的邮件，申明自己希望撤消证书。操作员打开邮件，填写 CRL 注册表，并且进行数字签名，提交给 CA，CA 操作员验证注册机构操作员的数字签名，批准用户撤消证书，并且更新 CRL，然后 CA 将不同格式的 CRL 输出给注册机构，公布到安全服务器上，这样其他人可以通过访问服务器得到 CRL。

证书撤销流程步骤如下。

（1）用户向注册机构操作员 CRLManager 发送一封签名加密的邮件，声明自己自愿撤销证书。

（2）注册机构同意证书撤销，操作员输入用户的序列号，对请求进行数字签名。

（3）CA 查询证书撤销请求列表，选出其中的一个，验证操作员的数字签名，如果正确，则同意用户的证书撤销申请，同时更新 CRL 列表，然后将 CRL 以多种格式输出。

（4）注册机构转发证书撤销列表。操作员导入 CRL，以多种不同的格式将 CRL 公布于众。

（5）用户浏览安全服务器，下载或浏览 CRL。

在一个 PKI，特别是 CA 中，信息的存储是一个非常核心的问题，它包括两个方面：一是 CA 服务器利用数据库来备份当前密钥和归档过期密钥，该数据库需高度安全和机密，其安全等级同 CA 本身相同；另外一个就是目录服务器，用于分发证书和 CRL，一般采用 LDAP 目录服务器。

4.9.3.4　密钥管理

密钥管理也是 PKI（主要指 CA）中的一个核心问题，主要是指密钥对的安全管理，

包括密钥产生、密钥备份、密钥恢复和密钥更新等。

（1）密钥产生。密钥对的产生是证书申请过程中重要的一步，其中产生的私钥由用户保留，公钥和其他信息则交于 CA 中心进行签名，从而产生证书。根据证书类型和应用的不同，密钥对的产生也有不同的形式和方法。对普通证书和测试证书，一般由浏览器或固定的终端应用来产生，这样产生的密钥强度较小，不适合应用于比较重要的安全网络交易。而对于比较重要的证书，如商家证书和服务器证书等，密钥对一般由专用应用程序或 CA 中心直接产生，这样产生的密钥强度大，适合于重要的应用场合。

另外，根据密钥的应用不同，也可能会有不同的产生方式。例如，签名密钥可能在客户端或 RA 中心产生，而加密密钥则需要在 CA 中心直接产生。

（2）密钥备份和恢复。在一个 PKI 系统中，维护密钥对的备份至关重要，如果没有这种措施，当密钥丢失后，将意味着加密数据的完全丢失，对于一些重要数据，这将是灾难性的。所以，密钥的备份和恢复也是 PKI 密钥管理中的重要一环。

使用 PKI 的企业和组织必须能够得到确认：即使密钥丢失，受密钥加密保护的重要信息也必须能够恢复，并且不能让一个独立的个人完全控制最重要的主密钥，否则将引起严重后果。

企业级的 PKI 产品至少应该支持用于加密的安全密钥的存储、备份和恢复。密钥一般用口令进行保护，而口令丢失则是管理员最常见的安全疏漏之一。所以，PKI 产品应该能够备份密钥，即使口令丢失，它也能够让用户在一定条件下恢复该密钥，并设置新的口令。

例如，在某些情况下用户可能有多对密钥，至少应该有两个密钥：一个用于加密，一个用于签名。签名密钥不需要备份，因为用于验证签名的公钥（或公钥证书）广泛发布，即使签名私钥丢失，任何用于相应公钥的人都可以对已签名的文档进行验证。但 PKI 系统必须备份用于加密的密钥对，并允许用户进行恢复，否则，用于解密的私钥丢失将意味着加密数据的完全不可恢复。

另外，使用 PKI 的企业也应该考虑所使用密钥的生命周期，它包括密钥和证书的有效时间，以及已撤消密钥和证书的维护时间等。

（3）密钥更新。对每一个由 CA 颁发的证书都会有有效期，密钥对生命周期的长短由签发证书的 CA 中心来确定，各 CA 系统的证书有效期限有所不同，一般大约为 2～3 年。

当用户的私钥被泄露或证书的有效期快到时，用户应该更新私钥。这时用户可以废除证书，产生新的密钥对，申请新的证书。

4.9.3.5 证书的使用与认证过程

在实际应用中，为了验证信息的数字签名，用户首先必须获取信息发送者的公钥证

书，以及一些额外需要的证书（如 CA 证书等，用于验证发送者证书的有效性）。

证书的获取可以有多种方式，如发送者发送签名信息时附加发送自己的证书，或以另外的单独信息发送证书，或者可以通过访问证书发布的目录服务器来获得，或者直接从证书相关的实体处获得。在一个 PKI 体系中，可以采取某种或某几种上述方式获得证书。

在电子商务系统中，证书的持有者可以是个人用户、企事业单位、商家和银行等。无论是电子商务中的哪一方，在使用证书验证数据时，都遵循同样的验证流程。一个完整的验证过程有以下几步。

（1）将客户端发来的数据解密（如解开数字信封）。

（2）将解密后的数据分解成原始数据、签名数据和客户证书三部分。

（3）用 CA 根证书验证客户证书的签名完整性。

（4）检查客户证书是否有效（当前时间在证书结构中所定义的有效期内）。

（5）检查客户证书是否作废（OCSP 方式或 CRL 方式）。

（6）验证客户证书结构中的证书用途。

（7）客户证书验证原始数据的签名完整性。

如果以上各项均验证通过，则接收该数据。

在 X.509 中，有三种认证过程以适应不同的应用环境：单向认证、双向认证和三向认证。可用图 4-111 简单表示。

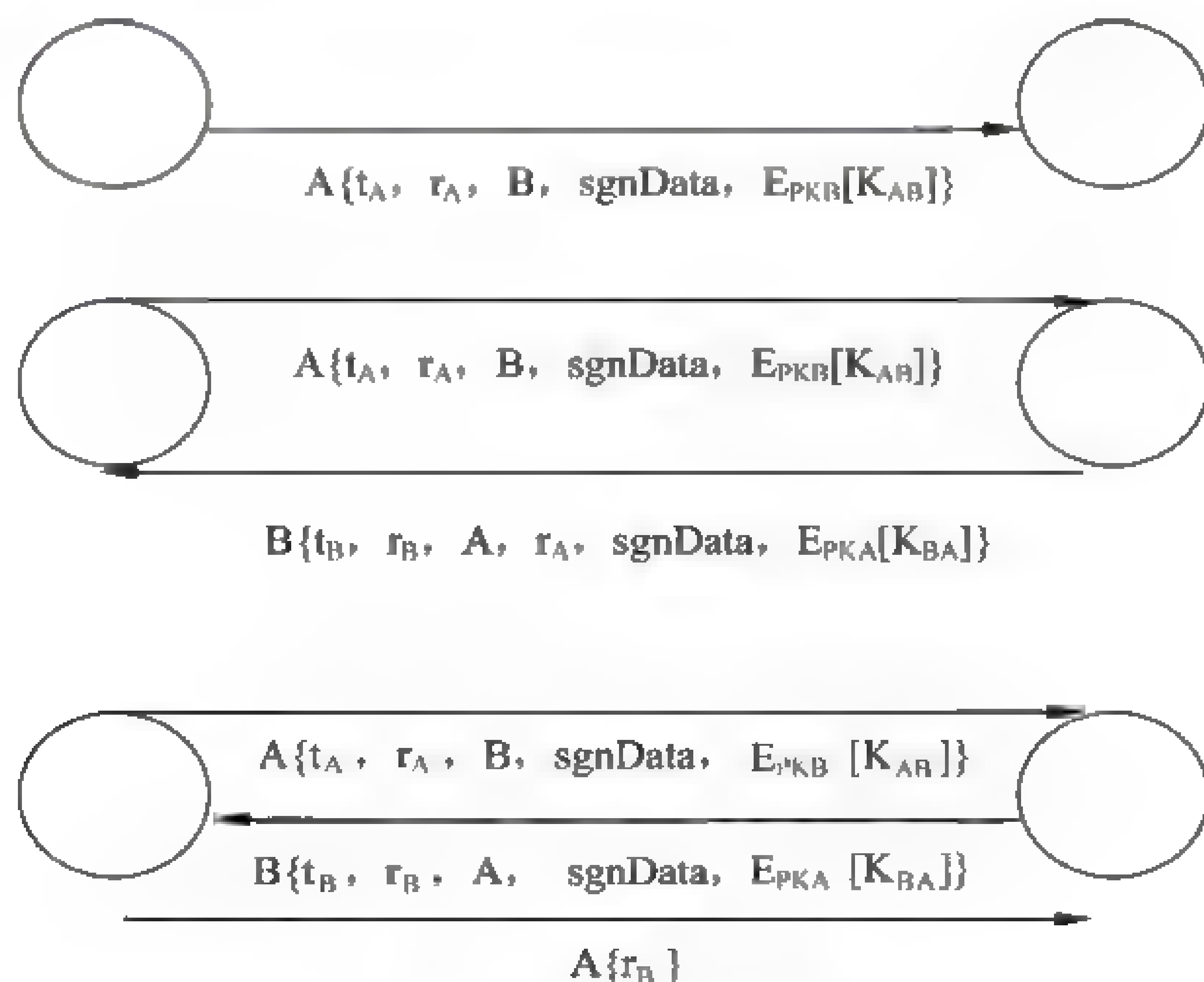


图 4-111　X.509 认证过程

其中，t_A 表示时间戳 A，r_A 表示一次性随机数，PKA 表示 A 的公开钥，K_{AB} 表示加密双方意欲建立的会话密钥，sgnData 表示其他信息。三种认证过程都使用公钥签名技

术，并假定通信双方都可从目录服务器获取对方的公钥证书，或对方最初发来的消息中包括公钥证书，即假定通信双方都知道对方的公钥。

4.9.4 PKI 和数字证书的应用

4.9.4.1 PKI 的应用实例

PKI 的应用非常广泛，包括在 Web 服务器和浏览器之间的通信、电子邮件、电子数据交换（EDI）、在 Internet 上的信用卡交易和虚拟私有网等。PKI 技术的广泛应用能满足人们对网络交易安全保障的需求。当然，作为一种基础设施，PKI 的应用范围在不断发展之中，下面给出几个应用实例。

（1）虚拟专用网络。VPN 是一种架构在公用通信基础设施上的专用数据通信网络，利用网络层安全协议（尤其是 IPSec）和建立在 PKI 上的加密与签名技术来获得机密性保护。基于 PKI 技术的 IPSec 协议现在已经成为架构 VPN 的基础，它可以为路由器之间、防火墙之间或者路由器和防火墙之间提供经过加密和认证的通信。虽然它的实现会复杂一些，但其安全性比其他协议都完善得多。

（2）安全电子邮件。作为 Internet 上最有效的应用，电子邮件凭借其易用、低成本和高效已经成为现代商业中的一种标准信息交换工具。随着 Internet 的持续增长，商业机构或政府机构都开始用电子邮件交换一些秘密的或是有商业价值的信息，这就引出了一些安全方面的问题，包括消息和附件可以在不为通信双方所知的情况下被读取、篡改或截掉；发信人的身份无法确认。电子邮件的安全需求也是机密、完整、认证和不可否认，而这些都可以利用 PKI 技术来获得。目前发展很快的安全电子邮件协议是 S/MIME（The Secure Multipurpose Internet Mail Extension），这是一个允许发送加密和有签名邮件的协议。该协议的实现需要依赖于 PKI 技术。

（3）Web 安全。浏览 Web 页面是人们最常用的访问 Internet 的方式。如果要通过 Web 进行一些商业交易，该如何保证交易的安全呢？为了透明地解决 Web 的安全问题，在两个实体进行通信之前，先要建立 SSL 连接，以此实现对应用层透明的安全通信。利用 PKI 技术，SSL 协议允许在浏览器和服务器之间进行加密通信。此外，服务器端和浏览器端通信时双方可以通过数字证书确认对方的身份。结合 SSL 协议和数字证书，PKI 技术可以保证 Web 交易多方面的安全需求，使 Web 上的交易和面对面的交易一样安全。

4.9.4.2 PKI 的应用编程接口

协议标准是系统具有可交互性的前提和基础，它规范了 PKI 系统各部分之间相互通信的格式和步骤。而应用编程界面（Application Programming Interface，API）则定义了如何使用这些协议，并为上层应用提供 PKI 服务。当应用需要使用 PKI 服务，如获取某一用户的公钥、请求证书废除信息或请求证书时都将会用到 API。目前 API 没有统一的

国际标准，大部分都是操作系统或某一公司产品的扩展，并在其产品应用的框架内提供 PKI 服务。

目前，有很多可以让开发者选择的 API 类型。IETF 建议标准为通用安全服务 API（Generic Security Service Application Program Interface，GSS-API），它提供了一种接口与网络机制和网络协议相互独立的实现。

欧洲建立的 SESAME（Secure European System for Application in a Multi-Vendor Environment）定义了一些安全界面，并作为该组织发展的安全技术的一部分，该接口得到了欧洲许多著名厂商的支持，如 Bull SA、ICL 和 Seimens 等，但没有在美国得到支持，特别是一些大的厂商，如 Microsoft 和 Netscape 等。

Entrust 也为其产品提供了一套 API，如 Entrust 证书管理服务 API（Entrust's Certificate Management Services API，CMS API），该 API 允许应用使用 Entrust 的证书管理和分发服务。在 1996 年指定，并于 1997 年更新的 PKIX Internet 草案 Architecture for Public Key Infrastructure 定义了 PKI 结构，并建议了许多标准，其中就包括 API。

目前，在 API 市场处于领先地位的是 Microsoft 的 CryptoAPI 和 Intel 的公用数据安全框架（Common Data Security Architecture，CDSA），他们凭借自己的产品优势相互竞争。Microsoft 利用其广泛的操作系统市场，而 Intel 则凭借其 PC 芯片的优势，并与其他厂商，如 IBM、Entrust 和 Netscape 等进行联合，共同支持 CDSA。现在也有很多厂商的 PKI 产品同时支持这两种 API，如 Entrust 等。PKIX 在很多情况下支持 CDSA，并建议其为 Architecture for Public Key Infrastructure 草案的标准。

除此之外，Entrust、IBM、Intel、Netscape 和 TIS 等联合向开放组织（Open Group）提议了一个基于 CDSA 的加密和证书管理接口，并使用了 Entrust 的 CMS API、IBM 的密钥恢复 API。但开放组织同时也在考虑使用 PKCS #11 作为安全 API 接口。

目前比较常用的安全 API 接口有 CryptoAPI（Microsoft Cryptographic Application Programming Interface，微软加密应用程序编程接口）和 CDSA（Common Data Security Architecture），CryptoAPI 为 Win32 应用程序提供了认证、编码、加密和签名等安全处理，它可使用户在对复杂的加密机制和加密算法不了解的情况下，对应用程序增加安全功能。

CDSA 为安全应用服务提供了一个整体框架和解决方案，提供了诸如证书管理等许多 PKI 功能。同 CryptoAPI 类似，CDSA 也是以一个分层的服务提供者框架为基础，其应用模式可分为 4 层。最上层是应用程序；应用程序的下层是中间件，例如 SSL、IPSec 接口和语言接口转换器等；接下来是 CSSM 层，CSSM 层是 CDSA 的核心层；CSSM 的下层是具体的服务提供者，如加密服务、证书服务、政策服务和数据存储服务等。

4.9.5　PKI 标准

PKI 发展的一个重要方面就是标准化问题，它也是建立互操作性的基础。PKI 的标

准可分为两个部分：一类用于定义 PKI；而另一类用于规范 PKI 的应用。

4.9.5.1 PKI 的定义标准

在 PKI 技术框架中，许多方面都经过严格的定义，如用户的注册流程、数字证书的格式、CRL 的格式、证书的申请格式以及数字签名格式等。PKI 的定义标准化有两大阵营：一是 RSA 公司的公钥加密标准（Public Key Cryptography Standards，PKCS），它定义了许多基本 PKI 部件，包括数字签名和证书请求格式等；二是由 Internet 工程任务组（Internet Engineering Task Force，IETF）和 PKI 工作组（Public Key Infrastructure Working Group，PKIX）所定义的一组具有互操作性的公钥基础设施协议。在今后很长的一段时间内，PKCS 和 PKIX 将会并存，大部分的 PKI 产品为保持兼容性，也将会对这两种标准进行支持。

1）X.209（1988）ASN.1 基本编码规则的规范

ASN.1 是描述在网络上传输信息格式的标准方法。它有两部分：第一部分（ISO 8824/ITU X.208）描述信息内的数据、数据类型及序列格式，也就是数据的语法；第二部分（ISO 8825/ITU X.209）描述如何将各部分数据组成消息，也就是数据的基本编码规则。

ASN.1 原来是作为 X.409 的一部分而开发的，后来才独立地成为一个标准。这两个协议除了在 PKI 体系中被应用外，还被广泛应用于通信和计算机的其他领域。

2）X.500（1993）信息技术之开放系统互联：概念、模型及服务简述

X.500 是一套已经被国际标准化组织（ISO）接受的目录服务系统标准，它定义了一个机构如何在全局范围内共享其名字和与之相关的对象。X.500 是层次性的，其中的管理性域（机构、分支、部门和工作组）可以提供这些域内的用户和资源信息。在 PKI 体系中，X.500 被用来唯一标识一个实体，该实体可以是机构、组织、个人或一台服务器。X. 500 被认为是实现目录服务的最佳途径，但 X.500 的实现需要较大的投资，并且比其他方式速度慢。而其优势是具有信息模型、多功能和开放性。

3）X.509（1993）信息技术之开放系统互联：鉴别框架

X.509 是由国际电信联盟（ITU-T）制定的数字证书标准。在 X.500 确保用户名称唯一性的基础上，X.509 为 X.500 用户名称提供了通信实体的鉴别机制，并规定了实体鉴别过程中广泛适用的证书语法和数据接口。国际电信联盟 ITU X.509 协议，是 PKI 技术体系中应用最为广泛、也是最为基础的一个国际标准。它的主要目的在于定义一个规范的数字证书的格式，以便为基于 X.500 协议的目录服务提供一种强认证手段。但该标准并非要定义一个完整的、可互操作的 PKI 认证体系。

X.509 的最初版本公布于 1988 年。X.509 证书由用户公共密钥和用户标识符组成。此外，还包括版本号、证书序列号、CA 标识符、签名算法标识、签发者名称和证书有效期等信息。这一标准的最新版本是 X.509 V3，它定义了包含扩展信息的数字证书。该版数字证书提供了一个扩展信息字段，用来提供更多的灵活性及特殊应用环境下所需的信

息传送。

4）PKCS 系列标准

由 RSA 实验室制订的 PKCS 系列标准，是一套针对 PKI 体系的加解密、签名、密钥交换、分发格式及行为标准，该标准目前已经成为 PKI 体系中不可缺少的一部分。PKCS 是由美国 RSA 数据安全公司及其合作伙伴制定的一组公钥密码学标准，其中包括证书申请、证书更新、证书作废表发布、扩展证书内容以及数字签名、数字信封的格式等方面的一系列相关协议。到 1999 年年底，PKCS 已经公布了以下标准。

- PKCS#1：定义 RSA 公开密钥算法加密和签名机制，主要用于组织 PKCS#7 中所描述的数字签名和数字信封。
- PKCS#3：定义 Diffie-Hellman 密钥交换协议。
- PKCS#5：描述一种利用从口令派生出来的安全密钥加密字符串的方法。使用 MD2 或 MD5 从口令中派生密钥，并采用 DES-CBC 模式加密。主要用于加密从一个计算机传送到另一个计算机的私人密钥，不能用于加密消息。
- PKCS#6：描述了公钥证书的标准语法，主要描述 X.509 证书的扩展格式。
- PKCS#7：定义一种通用的消息语法，包括数字签名和加密等用于增强的加密机制。PKCS#7 与 PEM 兼容，所以不需其他密码操作就可以将加密的消息转换成 PEM 消息。
- PKCS#8：描述私有密钥信息格式，该信息包括公开密钥算法的私有密钥以及可选的属性集等。
- PKCS#9：定义一些用于 PKCS#6 证书扩展、PKCS#7 数字签名和 PKCS#8 私钥加密信息的属性类型。
- PKCS#10：描述证书请求语法。
- PKCS#11：称为 Cyptoki，定义了一套独立于技术的程序设计接口，用于智能卡和 PCMCIA 卡之类的加密设备。
- PKCS#12：描述个人信息交换语法标准。描述了将用户公钥、私钥、证书和其他相关信息打包的语法。
- PKCS#13：椭圆曲线密码体制标准。
- PKCS#14：伪随机数生成标准。
- PKCS#15：密码令牌信息格式标准。

另外，PKCS#2 和 PKCS#4 已经合并到 PKCS#1 之中。PKIX 是由 IETF 组织中的 PKI 工作小组制定的系列国际标准，此类标准主要定义基于 X.509 和 PKCS 的 PKI 模型框架。PKIX 中定义的 4 个主要模型为用户、认证中心、注册中心和证书存取库。

5）OCSP 在线证书状态协议

OCSP（Online Certificate Status Protocol）是 IETF 颁布的用于检查数字证书在某一交易时刻是否仍然有效的标准。该标准提供给 PKI 用户一条方便快捷的数字证书状态查

询通道，使 PKI 体系能够更有效、更安全地在各个领域中被广泛应用。

6）LDAP 轻量级目录访问协议

LDAP 规范（RFC1487）简化了笨重的 X.500 目录访问协议，并且在功能性、数据表示、编码和传输方面都进行了相应的修改。1997 年，LDAP 第 3 版本成为互联网标准。目前，LDAP V3 已经在 PKI 体系中被广泛应用于证书信息发布、CRL 信息发布、CA 政策以及与信息发布相关的各个方面。

除了以上协议外，还有一些构建在 PKI 体系上的应用协议，这些协议是 PKI 体系在应用和普及化方面的代表作，包括 SET 协议和 SSL 协议。

4.9.5.2 PKI 的应用标准

PKI 的发展非常快，已经从几年前的理论阶段过渡到目前的产品阶段，并且出现了大量成熟技术、产品和解决方案，正逐步走向成熟。PKI 的发展受应用驱动的影响，例如，早期的 Internet 商务和 Web 安全要求主要依赖于 SSL，并要求应用首先对证书进行处理，所以，在很多公司的消息和群组产品中都提供了公钥和证书系统，如 Exchange 和 Notes 等。另外，基于标准的基础设施和应用也同样促进了 PKI 的发展，它能够保证基于 Internet 的安全消息传送的可交互性，如 S/MIME 等。

PKI 产品的生产厂家很多，比较有代表性的主要有 VeriSign 和 Entrust。VeriSign 作为 RSA 的控股公司，借助 RSA 成熟的安全技术，提供了 PKI 产品，为用户之间的内部信息交互提供安全保障。另外，VeriSign 也提供对外的 CA 服务，包括证书的发布和管理等功能，并且同一些大的生产商，如 Microsoft、Netscape 和 JavaSoft 等，保持了伙伴关系，以在 Internet 上提供代码签名服务。

Entrust 作为北方电信（Northern Telecom）的控股公司，从事 PKI 的研究与产品开发已经有很多年的历史了，并一直在业界保持领先地位，拥有许多成熟的 PKI 及配套产品，并提供了有效的密钥管理功能。

另外，一些大的厂商，如 Microsoft、Netscape 和 Novell 等，都开始在自己的网络基础设施产品中增加 PKI 功能。Netscape 已经开始把证书服务器作为 SuiteSpot 的一部分，虽然其证书服务器没有 Entrust 产品的功能全面和完善，但提供了基本的证书生成和管理功能。即使没有密钥管理功能，但由于 Netscape 把证书服务器同 SuiteSpot 服务器和 Communicator 客户端产品的集成，依靠广泛的市场基础，也取得了越来越多的市场份额。由 SUN 和 Netscape 联盟组成的 iplanet 公司（Sun|Netscape Alliance）也在 PKI 方面做了很大的努力，凭借其在网络和电子商务方面的优势，发展了很多性能优越的 PKI 产品，如 LDAP 目录服务器和证书管理系统等。

随着 PKI 的发展和应用的不断普及，PKI 的产品也越来越多，为了保持各产品之间的兼容性，标准化成了 PKI 不可避免的发展趋势。

目前世界上已经出现了许多依赖于 PKI 的安全标准，即 PKI 的应用标准，如安全的

套接层协议、传输层安全协议、安全的多用途因特网邮件扩展协议和 IP 安全协议等。

S/MIME 是一个用于发送安全报文的 IETF 标准。它采用了 PKI 数字签名技术并支持消息和附件的加密，无须收发双方共享相同密钥。S/MIME 委员会采用 PKI 技术标准来实现 S/MIME，并适当扩展了 PKI 的功能。目前该标准包括密码报文语法、报文规范、证书处理以及证书申请语法等方面的内容。

SSL/TLS 是因特网中访问 Web 服务器最重要的安全协议。当然，它们也可以应用于基于客户端/服务器模型的非 Web 类型的应用系统。SSL/TLS 利用 PKI 的数字证书来认证客户端和服务器的身份。

IPSec 是 IETF 制定的 IP 层加密协议，PKI 技术为其提供了加密和认证过程的密钥管理功能。IPSec 主要用于开发新一代的 VPN。

4.10　文件加密和电子签章

4.10.1　文件加密技术

文件加密是一种常见的密码学应用。文件加密技术是下面三种技术的结合。

（1）密码技术。包括对称密码和非对称密码，可能是分组密码，也可能采用序列密码，文件加密的底层技术是数据加密。

（2）操作系统。文件系统是操作系统的重要组成部分，对文件的输入输出操作或文件的组织和存储形式进行加密也是文件加密的常用手段。对动态文件进行加密尤其需要熟悉文件系统的细节。文件系统与操作系统其他部分的关联，如设备管理、进程管理和内存管理等，都可被用于文件加密。

（3）文件分析技术。不同的文件类型的语义操作体现在对该文件类型进行操作的应用程序中，通过分析文件的语法结构和关联的应用程序代码而进行一些置换和替换，在实际应用中经常可以达到一定的文件加密效果。

利用以上技术，文件加密主要包括以下内容。

（1）文件的内容加密，通常采用二进制加密的方法。

（2）文件的属性加密。

（3）文件的输入输出和操作过程的加密，即动态文件加密。

通常一个完整的文件加密系统包括操作系统的核心驱动、设备接口、密码服务组件和应用层几个部分。

4.10.2　EFS 文件加密技术

4.10.2.1　EFS 概述

通过文件加密，可以保护敏感数据。Windows Server 2003 通过登录认证和 NTFS 权

限可控制用户对文件的非授权存取，但如果用户在同一台计算机上安装并启动不同的操作系统，从而绕过登录认证和 NTFS 的权限设置，此时存放在硬盘上的数据就会变得非常脆弱。为消除这种安全漏洞，Microsoft 提供了加密文件系统（Encrypting File System，EFS），与 NTFS 紧密集成，给敏感数据提供深层保护。当文件被 EFS 加密后，只有加密用户和数据恢复代理用户才能解密加密文件，其他用户即使取得该文件的所有权也不能解密。

Microsoft 公司的 EFS 使用对称密钥和非对称密钥技术相结合的方法来提供文件的保护，对称密钥用于加密文件，非对称密钥中的公钥用于加密对称密钥。

在使用 EFS 时，EFS 首先检查用户是否有有效的 EFS 用户证书，如果没有，EFS 请求在线企业 CA 发布证书，如果企业 CA 不可得到，EFS 就为用户创建一个证书和用于以后 EFS 操作的公/私钥对。

EFS 加密发生在文件系统层而不在应用层，因此，其加密和解密过程对加密用户和应用程序是透明的。用户在使用加密文件时，感觉与普通文件一样。如打开文件调用 Win32 APIs 的 CreateFile 和 OpenFile 函数，读文件调用 ReadFile、ReadFileEx 和 Read-File Scatter 函数，写文件调用 WriteFile、WriteFileEx 和 WriteFileScatter 函数等。

4.10.2.2 EFS 的基本原理和结构

当用户生成加密文件时，随机密码产生器生成一个对称密钥 FEK，EFS 使用 FEK 加密文件中的数据，然后使用 EFS 用户证书中的公开密钥加密 FEK 得到数据解密域（Data Decryption Fields，DDF），再使用数据恢复代理（Data Recovery Agent，DRA）证书中的公钥加密 FEK。由于数据恢复代理可有多个，所以可能存在多个不同 DRA 证书中公钥加密的 FEK。所有这些经 DRA 证书中公钥加密的 FEK 组合在一起得到数据恢复域（Data Recovery Fields，DRF）。最后，EFS 将 DDF、DRF 作为加密文件头和经 FEK 加密的数据组合得到加密文件，其结构如图 4-112 所示。



图 4-112 EFS 加密文件的结构

为保证 EFS 系统对用户透明的操作，EFS 组件存在于操作系统的多个层上，主要分为用户模式和内核模式，用户模式主要包括 Win32 API 层、EFS 服务（EFS Service）、微软加密应用程序编程接口和加密服务提供者（Cryptographic Service Provider，CSP）。内核模式主要包括 EFS 驱动（EFS Driver）、EFS 文件系统运行库（File System Run-Time

Library，FSTRL），其关系如图 4-113 所示。

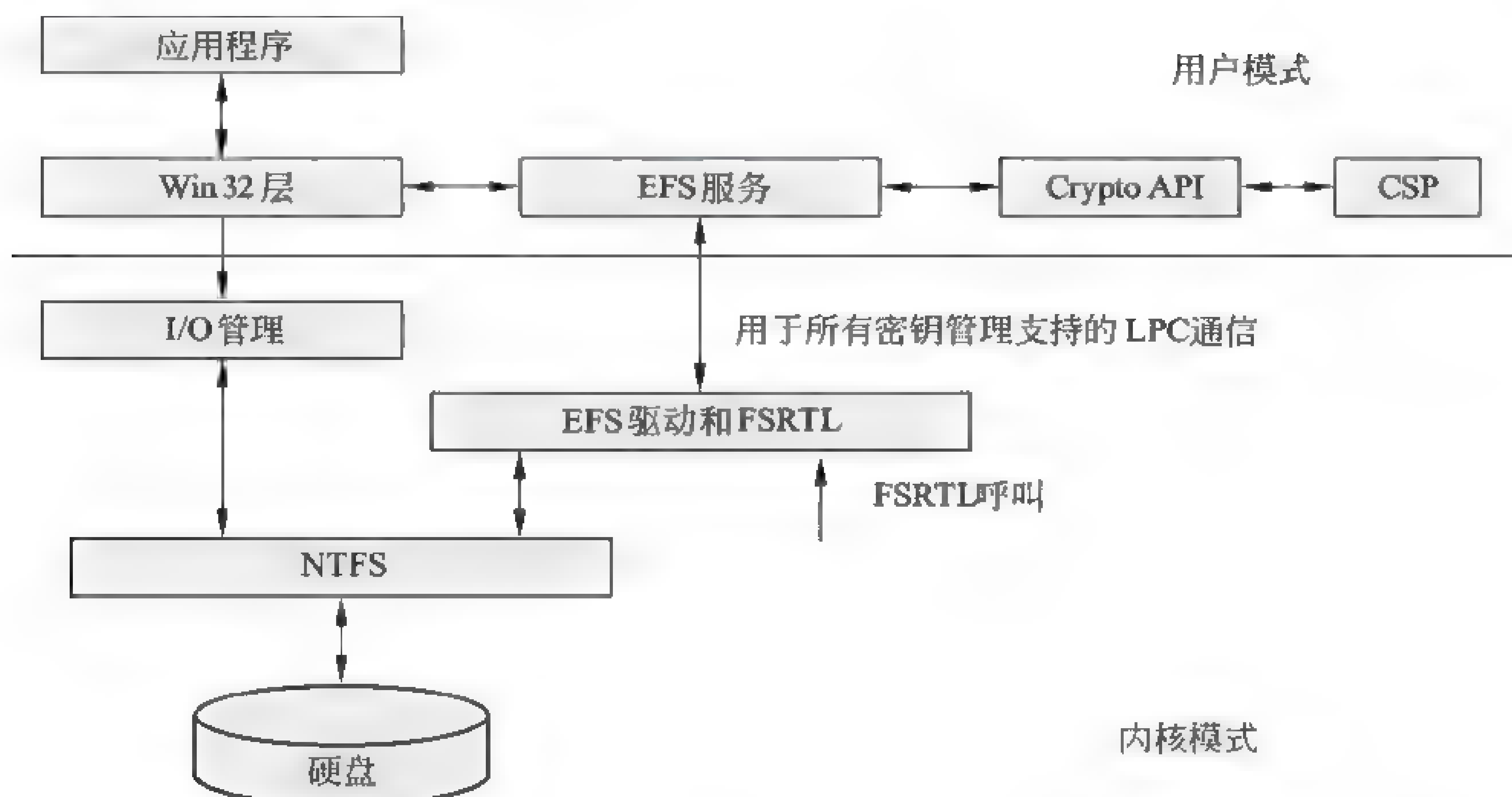


图 4-113　EFS 结构

（1）CSP。在 Windows Server 2003 中，EFS 使用默认的对称密钥加密算法 AES（Advanced Encryption Standard），其密钥长度达到 256 位，该加密强度足以保证一般用户的数据安全需求。在非对称密钥方面，EFS 默认使用 MicrosoftBase Provider，其默认密钥长度为 1024 位，可以通过修改以下注册表中的 DWORD 键值来增加加密强度：

HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\EFS\RSAKeyLength DWORD 键值的范围为 1024～16 384 位。要注意的是，如果设置值大于 1024，EFS 将使用 Microsoft Enhanced Provider 生成密钥。

（2）CryptoAPI。CryptoAPI 包含一组函数，并通过 EFS 服务为 Win32 层提供服务，包括公/私钥和对称密钥的密钥生成、密钥管理与密钥的安全存储、密钥交换、加密、解密、Hash 值计算、数字签名和签名验证等。在使用时，对 EFS 来说，CryptoAPI 中的所有操作是暗箱式的，EFS 只要调用相应函数来实现相应功能而不必关心实现的细节。

（3）Win32 层。Win32 层实质是一组 Win32 APIs，它为应用程序提供编程接口，如加密明文函数 EncryptFile()、解密密文函数 DecryptFile()、复制加密文件信息函数 DuplicateEncryption InfoFile()和加密文件状态函数 FileEncryptionStatus()等，这些函数的详细调用方法可参阅 MSDN Library for Visual Studio.NET 2003。所有的 Win32 API 由系统动态链接库 Advapi32.dll 提供。

（4）EFS 服务。EFS 服务调用 CryptoAPI 来为一个数据文件获得文件加密密钥，再调用 CryptoAPI 获得 EFS 用户证书中的公钥和 DRA 证书中的公钥，分别加密 FEK 形成 DDF 和 DRF。同时，通过本地过程调用 LPC（Local Procedure Call）通信模块与 EFS 驱

动传递 FEK、DDF 和 DRF。

（5）EFS 驱动。EFS 驱动与 NTFS 紧密集成，并位于 NTFS 逻辑上的最高层。EFS 驱动和 EFS 服务通信，请求 FEK、DDF 和 DRF，然后再把这些信息传递给 FSRTL 实现各种透明的文件操作，如打开文件、读文件和写文件等。

（6）EFS FSRTL。EFS FSRTL 实现由 NTFS 呼叫要求处理的各种文件系统操作，如读、写、打开加密文件和文件数据在写入或从磁盘中读出时的加密、解密及恢复数据等操作。在 EFS 结构中，EFS 驱动和 EFS FSRTL 以一个组件出现，但它们之间不直接通信，而是通过 NTFS 文件控制呼叫机制来彼此传递信息，这样确保了 NTFS 能参与到所有的文件操作中。通过 NTFS 文件控制呼叫机制实现的操作包括写 DDF、DRF 及传递在 EFS 服务中计算得到的 FEK 等。

4.10.2.3 EFS 加密解密文件的过程

EFS 本地加密文件的过程如下。

（1）EFS 服务调用 FileEncryptionStatus()确认文件是否可以加密，对系统文件和存放于%systemroot%文件夹中的文件不能被加密。若文件可加密，EFS 服务独占式地打开文件。

（2）EFS 服务调用 CryptoAPI 随机产生一个对称密钥 FEK。

（3）EFS 自动从用户证书中获取公钥并使用 RSA 加密算法加密 FEK 得到 DDF；EFS 自动从 DRA 证书中获取公钥并使用 RSA 加密算法加密 FEK，若有多个 DRA，则用每个 DRA 证书中的公钥加密 FEK 的每个备份，所有经 DRA 公钥加密后的 FEK 形成 DRF。其中，DRA 证书区别于 EFS 用户证书的标志是证书中的 EKU（Enhanced Key Usage）字段。所有的 DDF、DRF，再加上 EFS 版本信息和加密算法信息形成 EFS 元数据。

（4）EFS 在一个临时系统文件夹下建立一个临时文件，把要加密的源文件中所有数据流复制到临时文件。然后，EFS 将 EFS 元数据写入源文件，再将临时文件中的数据利用 FEK 通过 AES 加密算法逐块加密后形成加密块链附加到源文件，最后形成加密文件。因为元数据内容通常小于 1024 字节，而用 AES 加密算法加密数据后没有增加额外的数据，所以加密文件的大小与源文件相差无己。

（5）EFS 校验生成的加密文件，若校验成功，则删除临时文件。

当用户保存一个新文件到加密文件夹时，其过程除没有建立临时文件外，其余类似于上述过程。

EFS 本地解密文件的过程如下。

（1）NTFS 发送一个解密请求呼叫到 EFS 驱动。

（2）EFS 驱动从加密文件获得 DDF 并传递给 EFS 服务。

（3）EFS 服务从用户配置文件中获得用户的私钥解密 DDF 得到 FEK，再将 FEK 传递给 EFS 驱动。

（4）EFS 驱动使用 FEK 解密加密文件中应用程序需要的部分。要注意的是，因为 EFS 使用加密块链，所以 EFS 驱动只使用 FEK 解密应用程序需要的部分。

（5）EFS 驱动将解密后的数据传递到 NTFS，再由 NTFS 发送到应用程序。

4.10.3 电子印章的概念

电子签章（electronic signature）也叫电子签名。从法律的角度，所谓电子签章，是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。数据电文是指以电子、光学、磁或者类似手段生成、发送、接收或者储存的信息。我们平常所讲的数字签名属于电子签章中的一种，是指以非对称密钥技术为基础的签名，而电子签章还可以包括口令、密钥以及生物特征鉴别法等。

从技术的角度，电子印章泛指所有以电子形式存在，依附在电子文件并与其逻辑关联，可用以辨识电子文件签署者身份，保证文件的完整性，并表示签署者同意电子文件所陈述事实的内容。一般来说，对电子签章的认定，都是从技术角度而言的。主要是指通过特定的技术方案来鉴别当事人的身份及确保交易资料内容不被篡改的安全保障措施；从广义上讲，电子签章不仅包括我们通常意义上讲的数字签名，也包括计算机口令、生物笔迹辨别、指纹识别，以及新近出现的眼虹膜透视辨别法、面纹识别等。

电子签章系统是伴随着信息化建设而出现的高新技术。主要解决电子文件的签字盖章问题，用于辨识电子文件签署者的身份，保证文件的完整性，确保文件的真实性、可靠性和不可抵赖性。电子印章是一种用于电子文件之上，与传统的手写签名、盖章具有完全相同功能的技术。电子印章可以实现无纸化办公，有利于社会环境保护，减少自然资源浪费；并节约大量邮寄和传送费用；节省工作人员为盖章来回跑动的时间和精力。电子印章可存储于磁盘、IC 卡和 USB 存储棒等存储介质中。电子签章技术包括数字签章技术和逐渐普及的用于身份验证的生物识别技术如指纹、面纹和 DNA 技术等。目前，最成熟的电子签章技术是“数字签名（Digital Signature）”，它是以公钥及密钥的“非对称型”密码技术制作的电子签章。数字签章不是一个数字化的印章图片，并非是书面签字盖章的数字图像化，同时数字签章不是数字签名或数字签名的替代，更不是数字签名的增强，只是解决数字签名的可视化，是将传统的印鉴文化与现代密码学结合起来的一种技术。

利用电子签章，收件人能够通过网络传输文件并可以轻松验证发件人的身份和签章，还能验证出文件的原文在传输过程中有无变动。电子签章系统通过一套标准化、规范化的软硬结合的系统，使用户可以在电子文件上完成签字盖章，电子签章系统是电子时代的印章。

电子签名法的出台，为电子签章提供了技术和法律的保障。一旦发生了法律纠纷，可以根据电子签名追溯到责任人，并将之作为重要证据。电子签章问题也是电子商务和电子政务建设中必须首先解决的核心问题。我国的《电子签名法》规范了法律认可的数

据电文、数据电文的书面形式和原件形式的概念，同时解释了数据电文的文件保存以及作为证据的条件，明确了对数据电文的发送和收到的概念。

电子签名人是指持有电子签名制作数据并以本人身份或者以其所代表的人的名义实施电子签名的人；电子签名依赖方是指基于对电子签名认证证书或者电子签名的信赖从事有关活动的人；电子签名认证证书是指可证实电子签名人与电子签名制作数据有联系的数据电文或者其他电子记录；电子签名制作数据是指在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码等数据；电子签名验证数据是指用于验证电子签名的数据，包括代码、口令、算法或者公钥等。

在国外特别是西方，其电子公文中的公文认证和身份认证一般通过数字签名来实现。一个通用的数字签名系统包括两个功能模块：身份认证功能模块和内容认证功能模块。前者用来限制非法登录和用户权限的非法冒用，确保一个通信过程的合法性；后者用来保证合法通信过程中通信内容的可信性。

4.10.4 数字签名

4.10.4.1 可用的数字签名的条件

可用的数字签名应保证以下几个条件。

（1）签名是可信的。签名使文件的接收者相信签名者是慎重地在文件上签字的。

（2）签名不可伪造。签名证明是签字者而不是其他人慎重地在文件上签字。

（3）签名不可重用。签名是文件的一部分，不法之徒不可能将签名移到不同的文件上。

（4）签名的文件是不可改变的。在文件签名后，文件不能改变。

（5）签名是不可抵赖的。签名和文件是物理的东西。签名者事后不能声称他没有签过名。

在现实生活中，关于签名的这些特性没有一个是完全真实的。签名能够被伪造，签名能够从文章中盗用移到另一篇文章中，文件在签名后能够被改变。在计算机上做这种事情，同样存在一些问题。首先计算机文件易于复制。即使某人的签名难以伪造（例如，手写签名的图形），但是从一个文件到另一个文件剪切和粘贴有效的签名都是很容易的。这种签名并没有什么意义。其次，文件在签名后也易于修改，并且不会留下任何修改的痕迹。为解决这些问题，数字签名技术就应运而生。

4.10.4.2 对称密钥签名

Alice 想对数字消息签名，并送给 Bob。在 Trent 和对称密码系统的帮助下，她能对数字消息签名，并安全的送给 Bob。

Trent 是一个有权的、值得依赖的仲裁者。他能同时与 Alice 和 Bob（也可以是其他

想对数据文件签名的任何人）通信。他和 Alice 共享秘密密钥 KA，和 Bob 共享另一个不同的秘密密钥 KB。这些密钥在协议开始前就早已建好，并且为了多次签名可多次重复使用。

（1）Alice 用 KA 加密她准备发送给 Bob 的信息，并把它传送给 Trent。

（2）Trent 用 KA 解密信息。

（3）Trent 把这个解密信息和他收到 Alice 信息的声明，一起用 KB 加密。

（4）Trent 把加密的信息包传给 Bob。

（5）Bob 用 KB 解密信息包，他就能读 Alice 所发的信息和 Trent 的证书，证明信息来自 Alice。

整个过程如图 4-114 所示。

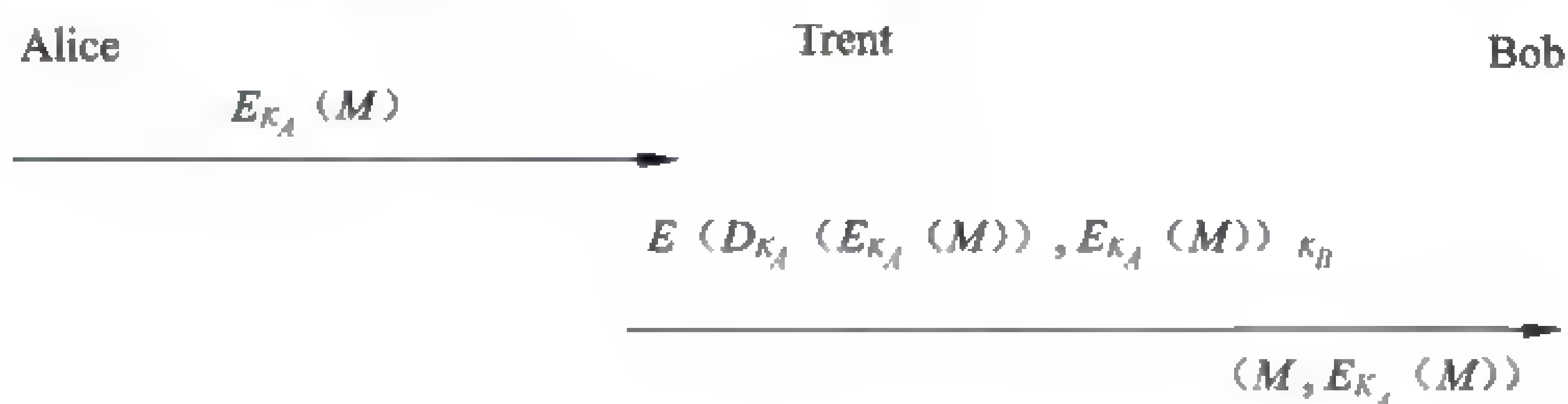


图 4-114　Alice 和 Bob 利用对称密钥签名进行的通信过程

Trent 怎么知道信息是从 Alice 而不是从其他人冒名顶替者那里来的呢？可以从信息的加密推断出来。由于只有他和 Alice 共享他们两人的秘密密钥，所以只有 Alice 能用这个密钥加密信息。

对该过程进行如下分析。

（1）这个签名是可信的，Trent 是可信的仲裁者，并且知道消息是从 Alice 那里来的，Trent 的证书对 Bob 起着证明的作用。

（2）这个签名是不可伪造的。只有 Alice（和 Trent，但每个人都相信他）知道 KA，因此只有 Alice 才能把用 KA 加密的信息传给 Trent。如果有人冒充 Alice，Trent 在第（2）步马上就会察觉，并且不会去证明它的可靠性。

（3）这个签名是不能重新使用的。如果 Bob 想把 Trent 的证书附到另一个信息上，Alice 可能就会大叫受骗了。仲裁者（可能是 Trent 或者可存取同一信息的完全不同的仲裁者）就会要求 Bob 同时提供信息和 Alice 加密后的信息，然后仲裁者就用 KA 加密信息，他马上就会发现它与 Bob 提供的加密信息不相同。很显然，Bob 由于不知道 KA，他不可能提供加密信息使它与用 KA 加密的信息相符。

（4）签名文件是不能改变的。Bob 想在接收后改变文件，Trent 就可用刚才描述的同样办法证明 Bob 的愚蠢行为。

（5）签名是不能抵赖的。如果 Alice 以后声称她没有发信息给 Bob，Trent 的证书会说明不是这样。因为 Trent 是每个人都信任的，他说的都是正确的。

如果 Bob 想把 Alice 签名的文件给 Carol 阅读，他不能把自己的秘密密钥交给她，还要通过 Trent。

（1）Bob 把信息和 Trent 关于信息是来自 Alice 的声明用 KB 加密，然后送回给 Trent。

（2）Trent 用 KB 解密信息包。

（3）Trent 检查他的数据库，并确认原始信息是从 Alice 那里来的。

（4）Trent 用他和 Carol 共享的密钥 KC 重新加密信息包，并把信息包送给 Carol。

（5）Carol 用 KC 解密信息包，她就能阅读信息和 Trent 证实信息来自 Alice 的证书。

这些协议是可行的，但对 Trent 来说是非常耗时的。他不得不整天加密、解密信息，在彼此想发送签名文件的每一对人之间充当中间人。他必须备有数据库信息（虽然可以通过把发送者加密的信息的备份发送给接收者来避免）。在任何通信系统中，即使他是毫无思想的软件程序，都是通信瓶颈。更困难的是，产生和保持像 Trent 那样的网络用户都信任的人。Trent 必须是完善无缺的，即使他在 100 万次签名中只犯了一个错误，也将不会有人再信任他。Trent 必须是完全安全的，如果他的秘密密钥数据库泄露了，或有人能修改他的程序代码，所有人的签名可能是完全无用的。一些声称是数年前签名的假文件便可能出现，这将引起混乱。理论上这种协议或许是可行的，但实际上不能很好运转。

4.10.4.3 公开密钥签名

在对称密码体制中由于加密密钥和解密密钥是可以相互推导的，密钥暴露会使系统变得不安全。对称密码体制的一个严重缺陷在于：通信双方在传送密文之前必须要使用一个安全信道预先通信密钥 K。在实际中找到一个满足要求的安全信道是很不容易的，一般都是通过物理方式交换密钥，如在约定地点秘密交换密钥。而公钥密码体制可以很容易地解决密钥交换问题。在公钥密码系统中，解密密钥和加密密钥是不同的，并且很难从一个推导出另外一个。公钥密码算法的密钥都是一对的，一个是私钥，用户自动保存并保密；另外一个是公钥，用户可以将它分发给任何需要的人。这样，通信双方不用预先交换密钥就可以建立保密通信了。

公开密钥签名的基本协议过程如下（如图 4-115 所示）。

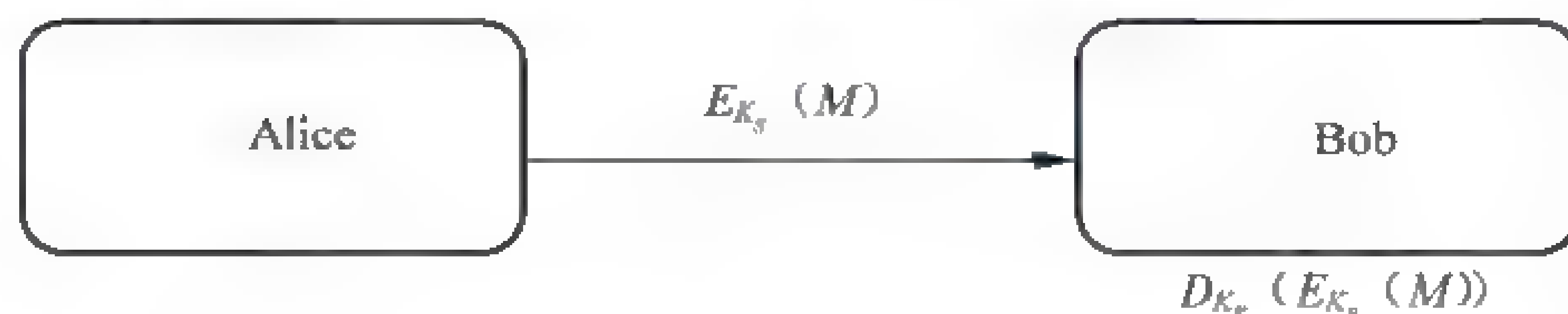


图 4-115　Alice 和 Bob 利用非对称密钥签名进行的通信过程

（1）Alice 用她的私钥对文件加密，从而对文件签名。

（2）Alice 将签名的文件传给 Bob。

（3）Bob 用 Alice 的公钥解密文件，从而验证签名。

这个协议比以前的算法更好。不需要 Trent 去签名和验证，他只需要证明 Alice 的公钥的确是她的。甚至协议的双方不需要 Trent 来解决争端，如果 Bob 不能完成第（3）步，那么他知道签名是无效的。

数字签名的基本过程如图 4-116 所示。这个协议也满足我们期待的特征。

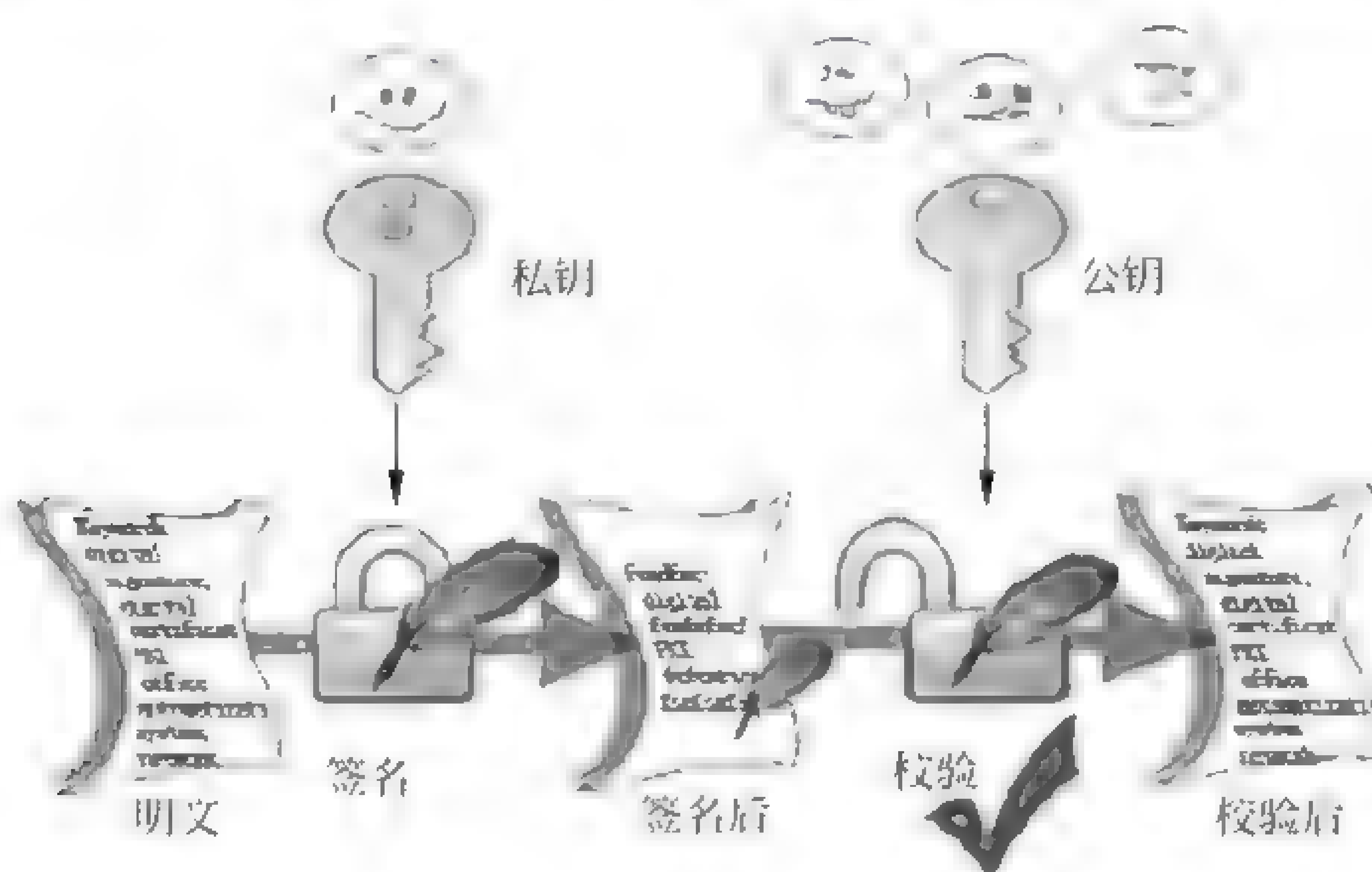


图 4-116 数字签名的基本过程

（1）签名是可信的。当 Bob 用 Alice 的公钥验证信息时，他知道是由 Alice 签名的。

（2）签名是不可伪造的。只有 Alice 知道她的私钥。

（3）签名是不可重用的。签名是文件的函数，并且不可能转换成另外的文件。

（4）被签名的文件是不可改变的。如果文件有任何改变，文件就不可能用 Alice 的公钥验证。

（5）签名是不可抵赖的。Bob 不用 Alice 的帮助就能验证 Alice 的签名。

4.10.4.4 基于消息摘要的签名

在实践中，采用公钥密码算法对长文件签名效率太低。为了节约时间，数字签名协议经常和单向 Hash 函数一起使用。Alice 并不对整个文件签名，只对文件的 Hash 值签名。在这个协议中，单向 Hash 函数和数字签名算法是事先就协商好了的。

（1）Alice 产生文件的单向 Hash 值。

（2）Alice 用她的私钥对 Hash 加密，凭此表示对文件签名。

（3）Alice 将文件和 Hash 签名送给 Bob。

（4）Bob 用 Alice 发送的文件产生文件的单向 Hash 值，然后用数字签名算法对 Hash 值运算，同时用 Alice 的公钥对签名的 Hash 解密。如果签名的 Hash 值与自己产生的 Hash 值匹配，签名就是有效的。

基于消息摘要的数字签名基本过程如图 4-117 所示。

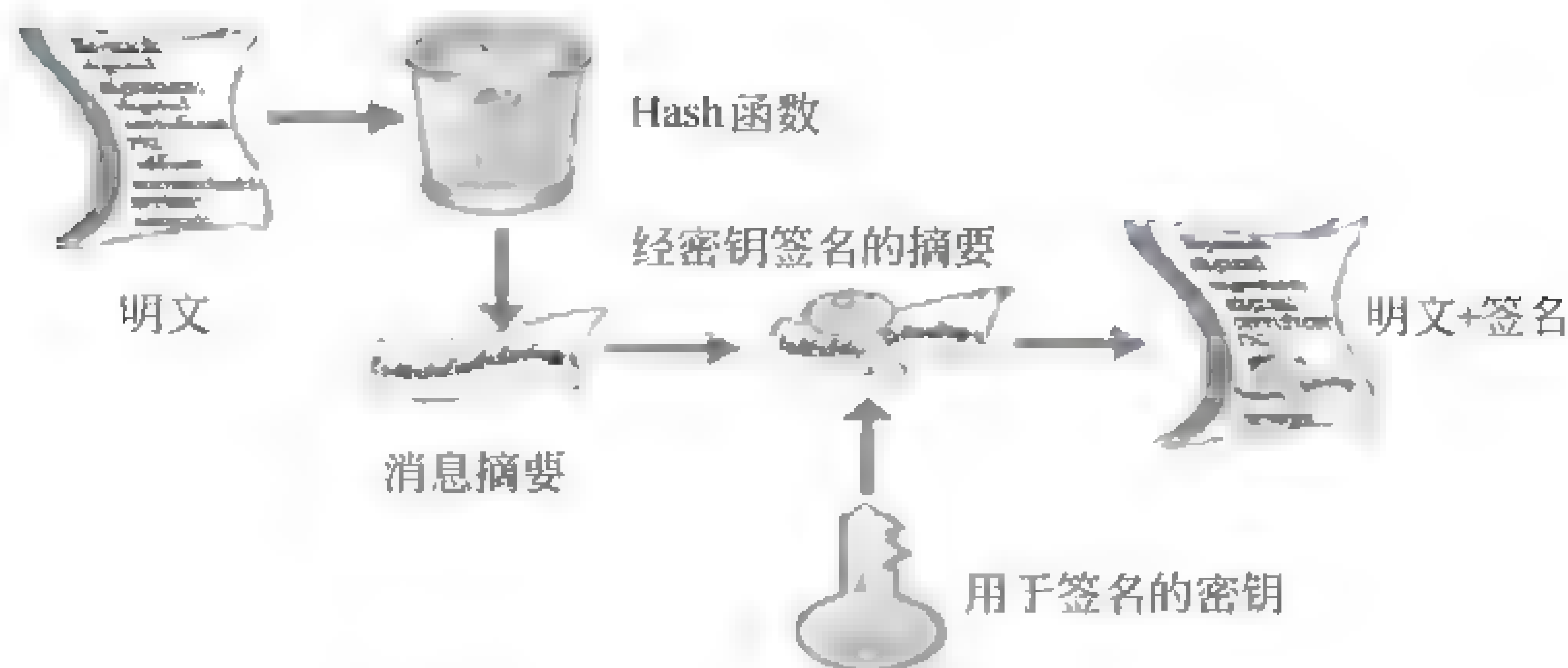


图 4-117　基于消息摘要的签名过程

计算速度大大地提高了，并且两个不同的文件有相同的 160 位 Hash 值的概率为 1/2。因此，使用 Hash 函数的签名和文件签名一样安全。如果使用非单向 Hash 函数，可能很容易产生多个文件使它们的 Hash 值相同，这样对一特定的文件签名就可复制用于对大量的文件签名。

该协议还有其他优点。首先，签名和文件可以分开保存。其次，接收者对文件和签名的存储量要求大大降低了。档案系统可用这类协议来验证文件的存在而不需保存它们的内容。中央数据库只存储各个文件的 Hash 值，根本不需要看文件。用户将文件的 Hash 值传给数据库，然后数据库对提交的文件加上时间标记并保存。如果以后有人对某文件的存在发生争执，数据库可通过找到文件的 Hash 值来解决争端。这里可能牵连到大量的隐秘：Alice 可能有某文件的版权，但仍保持文件的秘密。只有当她想证明她的版权时，她才不得不把文件公开。

4.10.5　电子印章的关键技术

在实践中，电子印章系统的主要技术包括 PKI 技术（或生物识别技术）、智能卡技术和数字水印技术。

当前的电子印章系统多是基于智能卡式的，智能卡是一种 IC 卡，具有一定的运算功能。用户的智能卡中存放有个人信息（图章或者签名信息）、证书信息以及密钥信息等，智能卡一般采用 PIN 码保护；用户在签章时需要提供自己的智能卡并提供自己的 PIN 码；此类型的电子印章系统由于其比较好的安全性、稳定性、方便性以及相对低廉的成本费用而得到比较普遍的应用。同时，当前的印章系统还有基于密码和生物测定式的。密码式电子印章系统要求用户设定一个密码，由数字和字符组成，来代表用户身份，也可以有相应的硬件设施（如电子笔）配合使用。此种电子印章系统不能对用户进行有效的管理，因而使用的范围比较小。

而生物测定式的电子印章系统是以用户的身体特征为基础，通过某种设备对用户的指纹、面部、视网膜或虹膜进行数字识别，从而确定对象是否与原使用者相同。此种电子签章系统由于要对持有者的某些身体特征进行采集，因而造成系统成本比较高，而且使用不方便，因而使用范围也比较有限。

基于生物识别技术，如指纹识别的电子印章系统，将指纹等信息以图形噪音的形式嵌入到印章图像中，并将印章图像与电子公文合并成特定格式文件，再通过专用打印机打印出来。这实际上是结合硬件实现的印章系统，包括专用的指纹采集器和专用的打印机，其缺点是以噪音的形式将信息嵌入到印章图像中必然导致印章图像质量的下降。

基于分布式简化严格层次（DSSH）PKI 信任结构类型的电子签章系统，将不同的实体划分在不同的域，每个域里只有一个认证中心，普通的 CA 之间通过中心 CA 进行交叉认证。通过数字签名保护印章的图形文件，并通过 IC 卡储存数字证书、印章文件及用户的私钥。

结合数字签名和数字水印技术的多媒体信息认证系统，通过数字签名实现发送方与接收方的身份认证，通过易碎数字水印来实现发送数据的完整性和真实性认证。

也有的技术方案将传统印章与电子印章进行结合，通过完整的印章网络管理系统，对于显式（可见）的传统印章，利用图像处理的若干技术，包括模板匹配、平滑和锐化等，识别印章图像。对于电子印章，将印章存到中心服务器，利用客户端/服务器或浏览器/服务器结构的系统进行访问。

在传统印章的电子鉴别方面的主要技术包括输入技术如扫描、数码照相等，识别技术如模板匹配、图像变换等。

4.10.6 数字水印技术

4.10.6.1 数字水印的概念和原理

信息安全技术大多以密码学理论为基础，无论是采用传统的密钥系统还是公钥系统，其保护方式都是控制文件的存取，即将文件加密成密文，使非法用户不能解读。但随着计算机处理能力的快速提高，这种通过不断增加密钥长度来提高系统密级的方法变得越来越不安全。另一方面，多媒体技术已被广泛应用，需要进行加密、认证和版权保护的声像数据也越来越多。数字化的声像数据从本质上说就是数字信号，如果对这类数据也采用密码加密方式，则其本身的信号属性就被忽略了。

数字水印是一种有效的数字产品版权保护和数据安全维护技术，是信息隐藏技术研究领域的一个重要分支，也是电子签章的主要技术之一。它用信号处理的方法在数字化的多媒体数据中嵌入隐蔽的标记，这种标记通常是不可见的，只有通过专用的检测器或阅读器才能提取。如果将具有特定意义的标记（水印），利用数字嵌入的方式隐藏在数字图像、声音、文档、图书和视频等数字产品中，即可用以证明创作者对其产品的所有权，

并作为鉴定、起诉非法侵权的证据，同时通过对水印的检测和分析来保证数字信息的完整可靠性，从而成为知识产权保护和数字多媒体防伪的有效手段。数字水印在版权保护、文件的真伪鉴别、网络的秘密通信、隐含标注和网络资源的安全等方面有着重要而广泛的应用。

数字水印技术的基本思想源于古代的密写术。古希腊的斯巴达人曾将军事情报刻在普通的木板上，用石蜡填平，收信的一方只要用火烤热木板，融化石蜡后，就可以看到密信。使用最广泛的密写方法恐怕要算化学密写了，牛奶、白矾和果汁等都曾充当过密写药水的角色。可以说，人类早期使用的保密通信手段大多数属于密写而不是密码。然而，与密码技术相比，密写术始终没有发展成为一门独立的学科，究其原因，主要是因为密写术缺乏必要的理论基础。

如今，数字化技术的发展为古老的密写术注入了新的活力，也带来了新的机会。在研究数字水印的过程中，研究者大量借鉴了密写技术的思想。尤其是近年来信息隐藏技术理论框架研究的兴起，更给密写术成为一门严谨的科学带来了希望。毫无疑问，密写技术将在数字时代得以复兴。

简单看来，水印系统包含水印嵌入模块和水印提取模块。水印嵌入模块的功能是完成将水印信号加入原始数据中；水印提取模块是用来判断某一数据块中是否含有特定的水印信号，并把该水印信号提取出来。图 4-118 表明了数字水印的生成和检测过程。

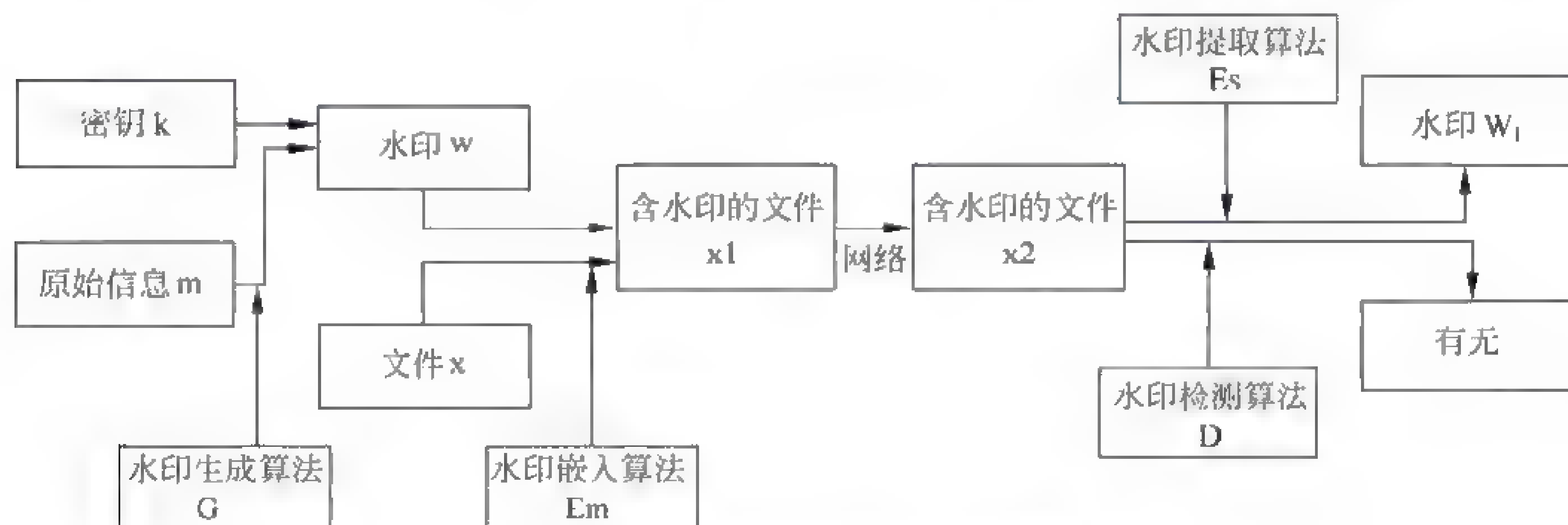


图 4-118 数字水印的生成和检测过程

4.10.6.2 数字水印的特征和分类

数字水印应具备以下几个特征。

（1）不可感知性，或隐蔽性。即嵌入的水印不会引起明显的降质，或数字产品在视觉或听觉质量上的下降，并且不易被察觉。

（2）隐藏位置的安全性。水印信息隐藏于数据而非文件头中，文件格式的变换不应导致水印数据的丢失。

（3）鲁棒性。所谓鲁棒性，是指在经历多种无意或有意的信号处理过程后，数字水印仍能保持完整性或仍能被准确鉴别。可能的信号处理过程包括信道噪声、滤波、数/模与模/数转换、重采样、剪切、位移、尺度变化以及有损压缩编码等。

在数字水印技术中，水印的数据量和鲁棒性构成了一对基本矛盾。从主观上讲，理想的水印算法应该既能隐藏大量数据，又可以抗各种信道噪声和信号变形。然而在实际中，这两个指标往往不能同时实现，不过这并不会影响数字水印技术的应用，因为实际应用一般只偏重其中的一个方面。如果是为了隐蔽通信，数据量显然是最重要的，由于通信方式极为隐蔽，遭遇敌方篡改攻击的可能性很小，因而对鲁棒性要求不高。但对保证数据安全来说，情况恰恰相反，各种保密的数据随时面临着被盗取和篡改的危险，所以鲁棒性是十分重要的，此时，隐藏数据量的要求居于次要地位。

数字水印技术可以从不同的角度进行划分。

（1）按特性划分。按水印的特性可以将数字水印分为鲁棒数字水印和脆弱数字水印两类。鲁棒数字水印主要用于在数字作品中标识著作权信息，如作者、作品序号等，它要求嵌入的水印能够经受各种常用的编辑处理；脆弱数字水印主要用于完整性保护，与鲁棒水印的要求相反，脆弱水印必须对信号的改动很敏感，人们根据脆弱水印的状态就可以判断数据是否被篡改过。

（2）按水印所附载的媒体划分。按水印所附载的媒体，可以将数字水印划分为图像水印、音频水印、视频水印、文本水印以及用于三维网格模型的网格水印等。随着数字技术的发展，会有更多种类的数字媒体出现，同时也会产生相应的水印技术。

（3）按检测过程划分。按水印的检测过程可以将数字水印划分为明文水印和盲水印。明文水印在检测过程中需要原始数据，而盲水印的检测只需要密钥，不需要原始数据。一般来说，明文水印的鲁棒性比较强，但其应用受到存储成本的限制。目前学术界研究的数字水印大多数是盲水印。

（4）按内容划分。按数字水印的内容可以将水印划分为有意义水印和无意义水印。有意义水印是指水印本身也是某个数字图像（如商标图像）或数字音频片段的编码；无意义水印则只对应于一个序列号。有意义水印的优势在于，如果由于受到攻击或其他原因致使解码后的水印破损，人们仍然可以通过视觉观察确认是否有水印。但对于无意义水印来说，如果解码后的水印序列有若干码元错误，则只能通过统计决策来确定信号中是否含有水印。在电子签章的应用中，大多数是有意义水印。

（5）按用途划分。不同的应用需求造就了不同的水印技术。按水印的用途，可以将数字水印划分为票据防伪水印、版权保护水印、篡改提示水印和隐蔽标识水印。

① 票据防伪水印。票据防伪水印是一类比较特殊的水印，主要用于打印票据和电子票据的防伪。一般来说，伪币的制造者不可能对票据图像进行过多的修改，所以，诸如尺度变换等信号编辑操作是不用考虑的。但另一方面，人们必须考虑票据破损、图案模糊等情形，而且考虑到快速检测的要求，用于票据防伪的数字水印算法不能太复杂。

② 版权标识水印。版权标识水印是目前研究最多的一类数字水印。数字作品既是商品又是知识作品，这种双重性决定了版权标识水印主要强调隐蔽性和鲁棒性，而对数据量的要求相对较小。

③ 篡改提示水印。篡改提示水印是一种脆弱水印，其目的是标识宿主信号的完整性和真实性。

④ 隐蔽标识水印。隐蔽标识水印的目的是将保密数据的重要标注隐藏起来，限制非法用户对保密数据的使用。

（6）按水印隐藏的位置划分。按数字水印的隐藏位置，可以将其划分为时（空）域数字水印、频域数字水印、时/频域数字水印和时间/尺度域数字水印。时（空）域数字水印是直接在信号空间上叠加水印信息，而频域数字水印、时/频域数字水印和时间/尺度域数字水印则分别是在 DCT 变换域、时/频变换域和小波变换域上隐藏水印。

随着数字水印技术的发展，各种水印算法层出不穷，水印的隐藏位置也不再局限于上述 4 种。应该说，只要构成一种信号变换，就有可能在其变换空间上隐藏水印。

4.10.6.3 数字水印的应用

数字水印作为电子印章的重要技术之一，可以应用于不同的领域。

1）数字作品的知识产权保护

数字作品（如电脑美术、扫描图像、数字音乐、视频和三维动画）的版权保护是当前的热点问题。由于数字作品的复制、修改非常容易，而且可以做到与原作完全相同，所以原创者不得不采用一些严重损害作品质量的办法来加上版权标志，而这种明显可见的标志很容易被篡改。

“数字水印”利用数据隐藏原理使版权标志不可见或不可听，既不损害原作品，又达到了版权保护的目的。目前，用于版权保护的数字水印技术已经进入了初步实用化阶段，IBM 公司在其“数字图书馆”软件中就提供了数字水印功能，Adobe 公司也在其著名的 Photoshop 软件中集成了 Digimarc 公司的数字水印插件。

2）商务交易中的票据防伪

随着高质量图像输入输出设备的发展，特别是精度超过 1200dpi 的彩色喷墨、激光打印机和高精度彩色复印机的出现，使得货币、支票以及其他票据的伪造变得更加容易。

据美国官方报道，仅在 1997 年截获的价值 4000 万美元的假钞中，用高精度彩色打印机制造的小面额假钞就占 19%，这个数字是 1995 年的 9.05 倍。目前，美国、日本以及荷兰都已开始研究用于票据防伪的数字水印技术。其中，麻省理工学院媒体实验室受美国财政部委托，已经开始研究在彩色打印机、复印机输出的每幅图像中加入唯一的、不可见的数字水印，在需要时可以实时地从扫描票据中判断水印的有无，快速辨识真伪。

另一方面，在从传统商务向电子商务转化的过程中，会出现大量过渡性的电子文件，如各种纸质票据的扫描图像等。即使在网络安全技术成熟以后，各种电子票据也还需要

一些非密码的认证方式。数字水印技术可以为各种票据提供不可见的认证标志，从而大大增加了伪造的难度。

3）声像数据的隐藏标识和篡改提示

数据的标识信息往往比数据本身更具有保密价值，如遥感图像的拍摄日期、经/纬度等。没有标识信息的数据有时甚至无法使用，但直接将这些重要信息标记在原始文件上又很危险。数字水印技术提供了一种隐藏标识的方法，标识信息在原始文件上是看不到的，只有通过特殊的阅读程序才可以读取。这种方法已经被国外一些公开的遥感图像数据库所采用。

此外，数据的篡改提示也是一项很重要的工作。现有的信号拼接和镶嵌技术可以做到“移花接木”而不为人知，因此，如何防范对图像、录音、录像数据的篡改攻击是重要的研究课题。基于数字水印的篡改提示是解决这一问题的理想技术途径，通过隐藏水印的状态可以判断声像信号是否被篡改。

4）隐蔽通信及其对抗

数字水印所依赖的信息隐藏技术不仅提供了非密码的安全途径，更引发了信息战尤其是网络情报战的革命，产生了一系列新颖的作战方式，引起了许多国家的重视。

网络情报战是信息战的重要组成部分，其核心内容是利用公用网络进行保密数据传送。迄今为止，学术界在这方面的研究思路一直未能突破“文件加密”的思维模式，然而，经过加密的文件往往是混乱无序的，容易引起攻击者的注意。网络多媒体技术的广泛应用使得利用公用网络进行保密通信有了新的思路，利用数字化声像信号相对于人的视觉、听觉冗余，可以进行各种时（空）域和变换域的信息隐藏，从而实现隐蔽通信。

4.10.7　密钥管理

4.10.7.1　密钥生成

密钥在概念上被分成两大类：数据加密密钥（DK）和密钥加密密钥（KK）。前者直接对数据进行操作，后者用于保护密钥，使之通过加密而安全传递。现实世界中，密钥管理是最困难的安全性问题。设计安全的密码算法和协议并非易事，但是保证密钥的安全却更为困难。密钥技术的核心内容是利用加密手段对大量数据的保护归结为对若干核心参量密钥的保护。密钥管理的任务综合了密钥的设置、产生、分配、注入、存储、传送、使用、注销和提取等一系列问题，它是信息安全的关键环节。

算法的安全性在于密钥。如果密钥由脆弱的密码程序生成，那么整个系统都将处于极其脆弱的环境中，当攻击者能够分析密钥生成算法时，也就无须分析密码算法了。

密钥生成需要考虑如下三个方面的因素。

1）增大密钥空间

一个密码算法的密钥若设为 N 位，那么该密钥空间为 2N 个。显然，若某加密程序

限制了密钥的位数，那么密钥空间随之减小，特别是当密钥生成程序比较脆弱，将导致密钥能够轻易被破译。例如，采用各种专用蛮力攻击硬件和并行技术，无论是对于一台机器甚至是多台机器并行处理，只要每秒测试 100 万个密钥，破译 8 字节以下小写字母和小写字母与数字构成的密钥、7 字节以下字母数字密钥、6 字节以下可打印字母密钥和 ASCII 字符密钥以及 5 字节以下 8 位的 ASCII 字符密钥都是可以的。另外，随着计算机设备的不断改进，对破译的时间和条件要求也越来越少。

但是反过来想，只要我们加长密钥位数，增大密钥空间，对阻止攻击是很有帮助的。例如，采用穷举搜索所有密钥的时间，对于 8 位 ASCII 字符（256 个）在 4 字节密钥空间下只需要 1.2 小时，在 6 字节密钥空间下需要 8.9 年，而在 8 字节情况下需要 580 000 年。这明显增加了攻击的难度。

2）选择强钥

在实际应用中，人们为了能方便记忆，往往选择较弱的密钥，如选择 Klone，而不是“*9（hH\A-”。简单的密钥方便了人们的记忆，也方便了攻击者的测试。对于公钥算法，不同的算法对强钥的选择也有不同的规定。

3）密钥的随机性

好的生成密钥是一个随机位串。会话密钥的产生，用随机数作为会话密钥；公钥密码算法也采用随机数作为密钥。密钥位可从可靠的随机源获得，如一些物理噪声产生器、离子辐射脉冲检测器、气体放电关和漏电容等；也可从安全的伪随机数发生器借助于安全的密码算法来产生，只要设计得好，能通过各种随机性检验就具有伪随机性。

随机数序列需满足随机性和不可预测性的要求。首先，均匀分布和独立性可以用来保证随机数的随机性，数列中每个数的出现频率应基本相等且均不能由其他数推出。在设计密码算法时，经常会使用一种称为伪随机数列的数列。例如，在 RSA 算法中素数的产生。一般情况下，决定一个大数 N 是否为素数是很困难的。最原始的方法就是用每个比 N 的 $\frac{1}{2}$ 小的数去除 N，如果 N 很大，比如 10 160，这一方法则超出人类的分析能力和计算能力。另外，在相互认证和会话密钥的产生等应用中，更要求数列中以后的数是不可预测的。

4.10.7.2 对称密钥分配

密钥分配一般要解决两个问题：一是引进自动分配密钥机制，以提高系统的效率；二是尽可能减少系统中驻留的密钥量。这两个问题也可以同步解决。

1）密钥的使用控制

两个用户（主机、进程、应用程序）在进行保密通信时，必须拥有一个共享的并且经常更新的秘密密钥。密钥的分配技术从一定程度上决定着密码系统的强度。

控制密钥的安全性主要有以下两种技术。

（1）密钥标签。例如用于 DES 的密钥控制，将 DES 中的 8 个校验位作为控制这个密钥的标签，其中前三位分别代表了该密钥的不同信息：主/会话密钥、加密和解密。但是长度过于限制，且须经解密方能使用，带来了一定的不便性。

（2）控制矢量。被分配的若干字段分别说明不同情况下密钥是被允许使用或者不允许，且长度可变。它在密钥分配中心（Key Distribution Center，KDC）产生密钥时加在密钥之中：首先由一杂凑函数将控制矢量压缩到加密密钥等长，然后与主密钥异或后作为加密会话密钥的密钥，即

$H = h（CV）$

$K_{in} = K_m \text{ XOR } H$

$K_{out} = E_{Km \text{ XOR } H}[K_S]$

其恢复过程为 $K_S = D_{Km \text{ XOR } H}[E_{Km \text{ XOR } H}[K_S]]$。

用户只有使用与 KDC 共享的主密钥以及 KDC 发送过来的控制矢量才能恢复会话密钥，因此，须保证保留会话密钥和他控制矢量之间的对应关系。

2）密钥的分配

两个用户 A 和 B 在获得共享密钥时可以有 4 种方式。

（1）经过 A 选取的密钥通过物理手段发送给另一方 B。

（2）由第三方选取密钥，再通过物理手段分别发送给 A 和 B。

（3）A、B 事先已有一密钥，其中一方选取新密钥后，用已有密钥加密该新密钥后发送给另一方。

（4）A、B、C 三方各有一保密信道，C 选取密钥后，分别通过 A、B 各自的保密信道发送。

前两种方法称为人工发送。若网络中 N 个用户都要求支持加密服务，则任意一对希望通信的用户各需要一个共享密钥，这导致密钥数目多达 $N（N-1）/2$。第三种方法，攻击者一旦获得一个密钥就可获取以后所有的密钥，这就给安全性带来隐患。这三种方法的公共弱点在于当 N 很大时，密钥的分配代价也变得非常大。但是，这种无中心的密钥控制技术在整个网络的局部范围内却显得非常有用。如图 4-119 所示，N 表示随机数。

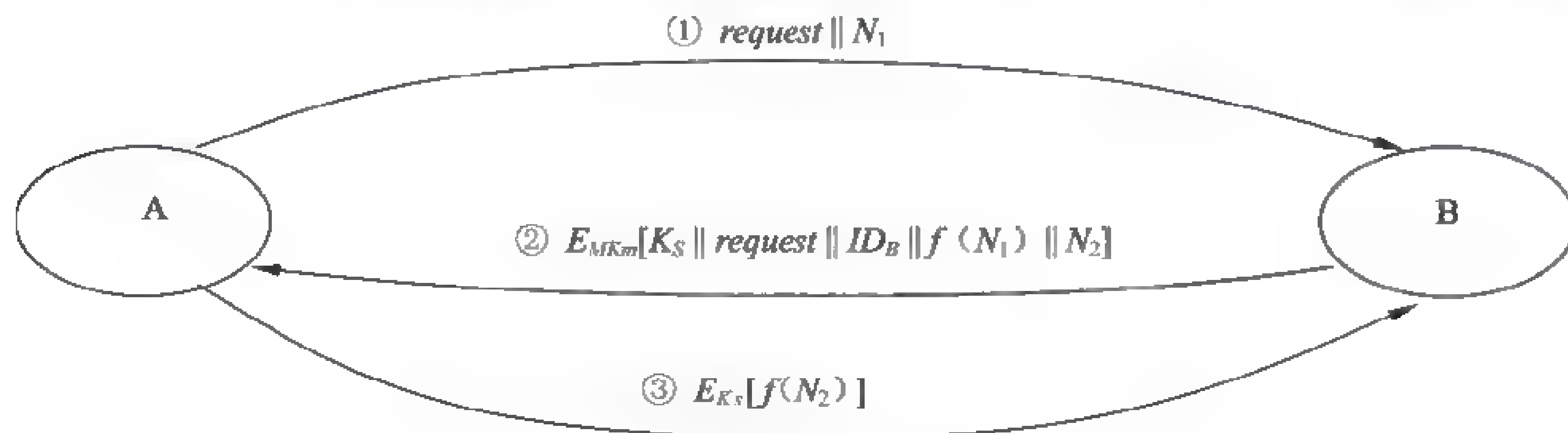


图 4-119　无 KDC 的密钥分配

第四种方法是较常用的。第三方 C 是为用户分配密钥的 KDC，每个用户和 KDC 有一个共享密钥，即主密钥。主密钥再分配给每对用户会话密钥，用于用户间的保密通信。会话密钥在通信结束后立即销毁。虽然此种方法的会话密钥数目是 $N（N-1）/2$，但是主密钥的数目却只需要 N 个，可以通过物理手段进行发送。如图 4-120 所示，N 表示随机数，K_s 表示会话密钥。

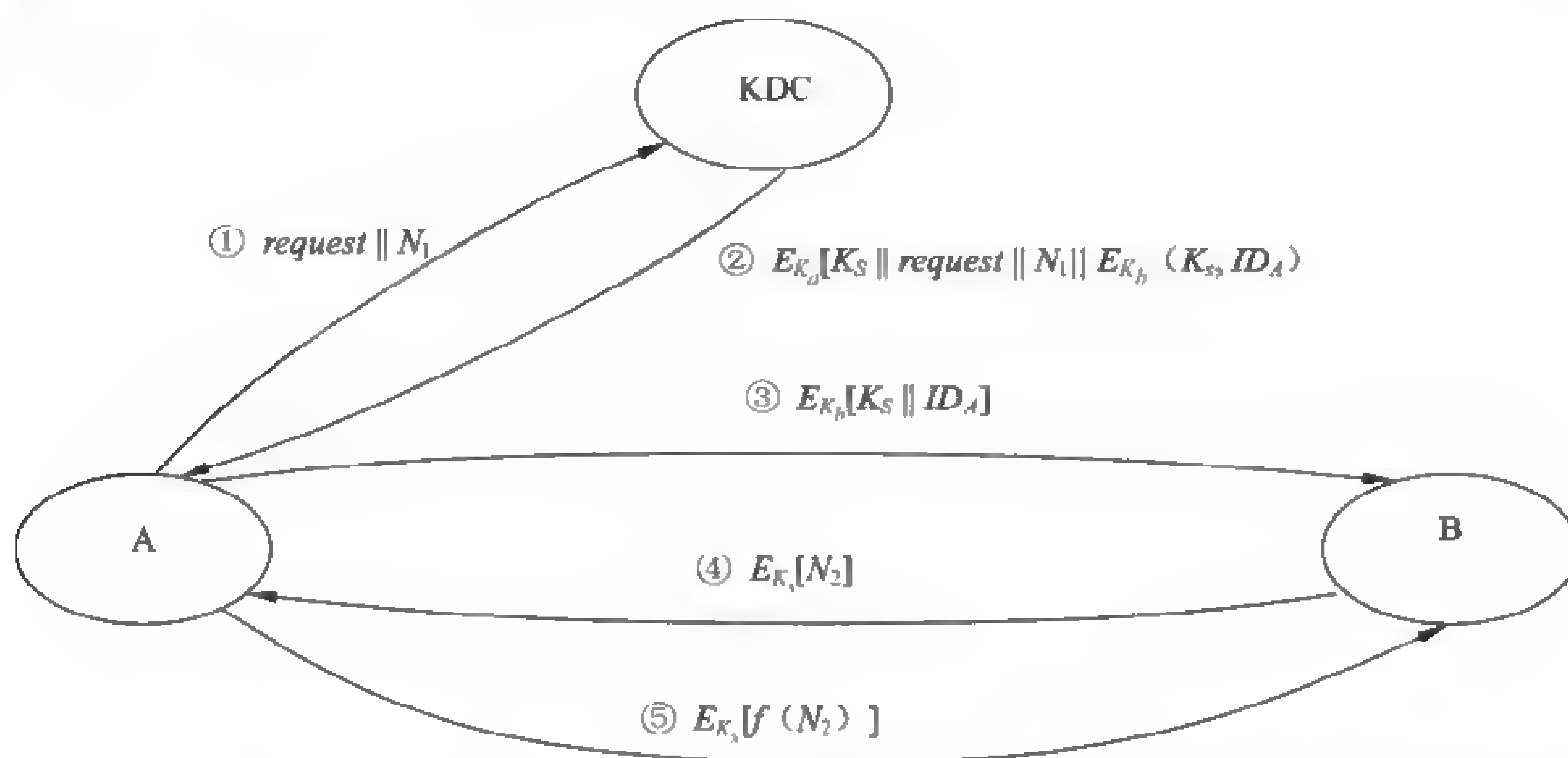


图 4-120 有 KDC 的密钥分配

由于网络中用户数目非常多并且地域分布非常广泛，因此有时需要使用多个 KDC 的分层结构。可在每个小范围（如一个 LAN 或一个建筑物）内建立本地 KDC，不同范围的两个本地间可再用一个全局 KDC 连接。这样建立的两层 KDC 不但减少了主密钥的分布，更可以将虚假的 KDC 的危害限制到一个局部的区域。

另外，应注意会话密钥有效期的设置。会话密钥更换得越频繁，系统的安全性也就越高。但是另一方面，频繁更换会话密钥会造成网络负担，延迟用户之间的交换。因此在决定其有效期时，应权衡矛盾的两个方面。

4.10.7.3 公钥加密体制的密钥管理

公钥密码体制采用的是公开加密密钥，而解密密钥只有通信双方通过某些途径才能得知。

（1）公开发布。公开发布是指用户将自己的公钥发给每一个其他用户，或向某一团体广播。这种方法虽然简单，但有一个非常大的缺点：任何人都可以伪造这种公开发布。如果某个用户假装是用户 A 并以 A 的名义向另一个用户发送或广播自己的公开钥，则在 A 发现假冒者以前，这一假冒者可解读所有发向 A 的加密消息，甚至还能用伪造的密钥获得认证。

PGP（pretty good privacy）中采用 RSA 算法，很多用户就可将自己的公钥附加到消

息上，发送到公开区域。

（2）公用目录表。公用目录表是指一个公用的公钥动态目录表，由某个可信的实体或组织（公用目录的管理员）承担该公用目录表的建立、维护以及公钥的分布等。管理员为每个用户在目录表中建立一个目录，其中包括用户名和用户的公开钥两个数据项，并且定期公布和更新目录表。每个用户都亲自或以某种安全的认证通信在管理者那里注册自己的公开钥，可通过电子手段访问目录表，还可随时替换新密钥。但是，这种公用目录表的管理员秘密钥一旦被攻击者获取，同样面临被假冒的危险。

（3）公钥管理机构。与公用目录表类似，用公钥管理机构来为各用户建立、维护动态的公钥目录，这种对公钥分配更加严密的控制措施可以增强其安全性。特别注意的是，每个用户都可靠地知道管理机构的公开钥，但是只有管理机构自己知道相应的秘密钥。

例如，当用户 A 向公钥管理机构发送一个请求时，该机构对请求作出应答，并用自己的秘密钥 SKAU 加密后发送给 A，A 再用机构的公开钥解密。

它的缺点在于因为每一个用户要想和他人联系都需求助于管理机构，所以容易使管理机构成为系统的瓶颈，并且管理机构维护的公钥目录表也容易被敌手窜扰。

（4）公钥证书。公钥证书可以从一定程度上解决以上策略存在的一些不足之处。公钥证书是由证书管理机构为用户建立的，其中的数据项有与该用户的秘密钥相匹配的公开钥及用户的身份和时戳等，所有的数据项经 CA 用自己的秘密钥签字后就形成证书，即证书的形式为 CA=ESKCA[T，IDA，PKA]。T 是当前的时戳，IDA 是用户 A 的身份，PKA 是 A 的公钥，SKCA 是 CA 的秘密钥，CA 则是用户 A 产生的证书。

用户将自己的公开钥通过公钥证书发给另一个用户，而接收方则可用 CA 的公钥 PKCA 对证书加以验证。这样，通过证书交换用户之间的公钥而无须再与公钥管理机构联系，从而避免了由统一机构管理所带来的不便和安全隐患。

4.10.7.4　公钥加密分配单钥密码体制的密钥

公开钥分配完之后，用户可用公钥加密体制进行保密通信。但是，这种加密体制的加密速度比较慢，因此比较适合于单钥密码体制的密钥分配，如图 4-121 所示。

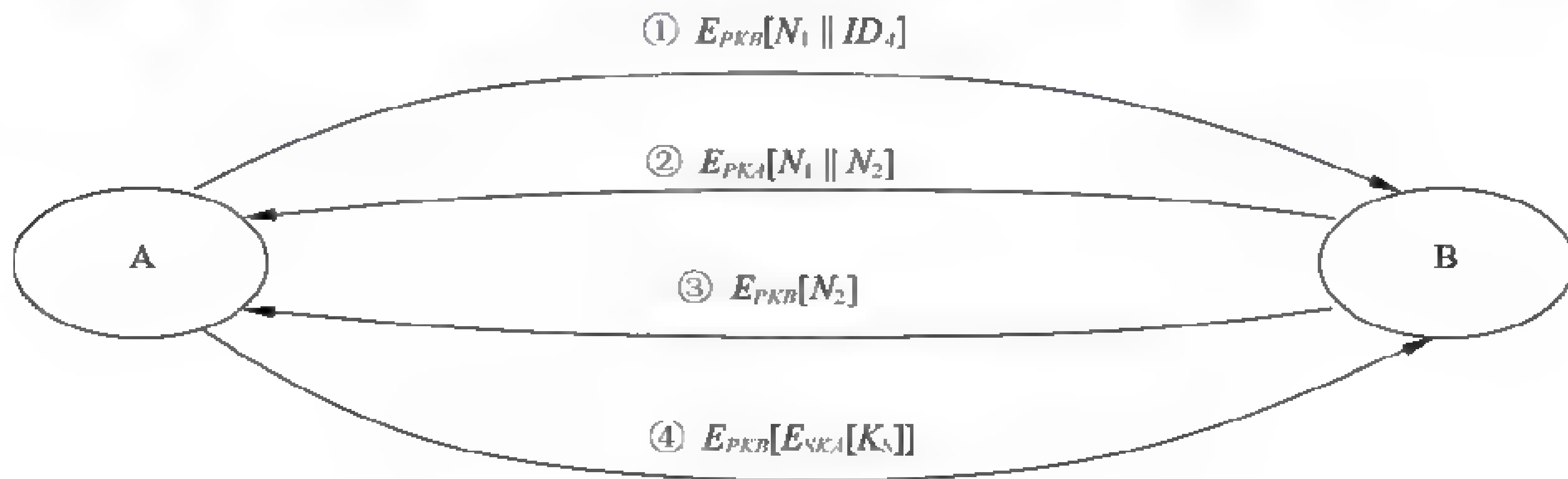


图 4-121　密钥分配

假定 A、B 双方用户已完成公钥交换，则可利用公钥加密体制按照如上步骤建立共享会话密钥。

（1）A 将用 B 的公钥加密得到的身份 ID_A 和一个用于唯一标志这个业务的一次性随机数 N_1 发往 B。

（2）预使 A 确定对方是 B，则 B 用 A 的公钥加密 N_1 和另一新产生的随机数 N_2，因为只有 B 能解读（1）中的加密。

（3）A 用 B 的公钥 PK_B 对 N_2 加密后返回给 B，以使 B 相信对方确是 A。

（4）A 将 $M = E_{PKB}[E_{SKA}[K_S]]$发送给 B，其中 K_S 为会话密钥，用 B 的公开钥加密是为保证只有 B 能解读加密结果，用 A 的秘密钥加密是保证该加密结果只有 A 能发送。

（5）B 以 $D_{PKA}[D_{SKB}[M]]$ 恢复会话密钥。

这种分配过程的保密性和认证性均非常强，既可防止被动攻击，又可防止主动攻击。

4.11 网络安全应用协议

4.11.1 SSL 协议

4.11.1.1 SSL 协议概述

SSL 协议是网景公司提出的基于 Web 应用的安全协议。SSL 协议指定了一种在应用层协议和 TCP/IP 协议之间提供数据安全性分层的机制，它为 TCP/IP 连接提供数据加密、服务器认证、消息完整性以及可选的客户机认证，可以在两个通信应用程序之间提供数据的加密性和可靠性。SSL 能在 TCP/IP 和应用层间无缝实现 Internet 协议栈处理，而不对其他协议层产生任何影响。

1995 年，Netscape 公司提出了 SSL 2.0 之后，很快就成为一个事实上的标准，并被众多的厂商所采用。1996 年，Netscape 公司发布了 SSL 3.0，该版本增加了对除了 RSA 算法之外的其他算法的支持和一些安全特性，并且修改了前一个版本中一些小的问题，相比 SSL 2.0 更加成熟和稳定。1999 年 1 月，IETF（www.ietf.org）将 SSL 作了标准化，即 RFC 2246，Netscape 公司宣布支持该开放的标准。在 WAP 的环境下，由于手机及手持设备的处理和存储能力有限，wap 论坛（www.wapforum.org）在 TLS 的基础上做了 WTLS 协议（Wireless Transport Layer Security），以适应无线的特殊环境。

SSL 协议提供的安全连接具有以下几个基本特性。

（1）连接安全。在初始化握手结束后，SSL 使用加密方法来协商一个秘密的密钥，数据加密使用对称密钥技术（如 DES、RC4 等）。

（2）身份认证。可以通过非对称（公钥）加密技术（如 RSA、DSA 等）认证对方的身份。

（3）可靠性连接。传输的数据包含有数据完整性的校验码，使用安全的哈希函数（如

SHA、MD5 等）计算校验码。

SSL 协议主要包括记录协议、告警协议和握手协议。

4.11.1.2　SSL 记录协议

SSL 本身是一个分层协议，每一层的消息块都包含有长度、描述和内容。SSL 在传输前将消息打包成消息块，在此过程中可进行压缩、生成 MAC 和加密等。接收方则对消息块进行解压、MAC 验证和解压，并进行重装配，再传给上一层。这些是通过记录协议层来规定的。SSL 协议的记录协议层在客户端和服务器之间传输应用数据和 SSL 控制数据，即用于交换应用数据，包括了记录头和记录数据格式的规定。在 SSL 协议中，所有的传输数据都被封装在记录中。记录是由记录头和长度不为 0 的记录数据组成的。SSL 的记录数据包含三个部分：MAC 数据、实际数据和粘贴数据。所有的 SSL 通信包括握手消息、安全空白记录和应用数据都使用 SSL 记录层。应用程序消息被分割成可管理的数据块，还可以压缩，并产生一个 MAC（消息认证代码），然后将结果加密并传输。接收方接收数据并对它解密，校验 MAC，解压并重新组合，再把结果提供给应用程序协议。

SSL 记录协议的操作过程如图 4-122 所示。

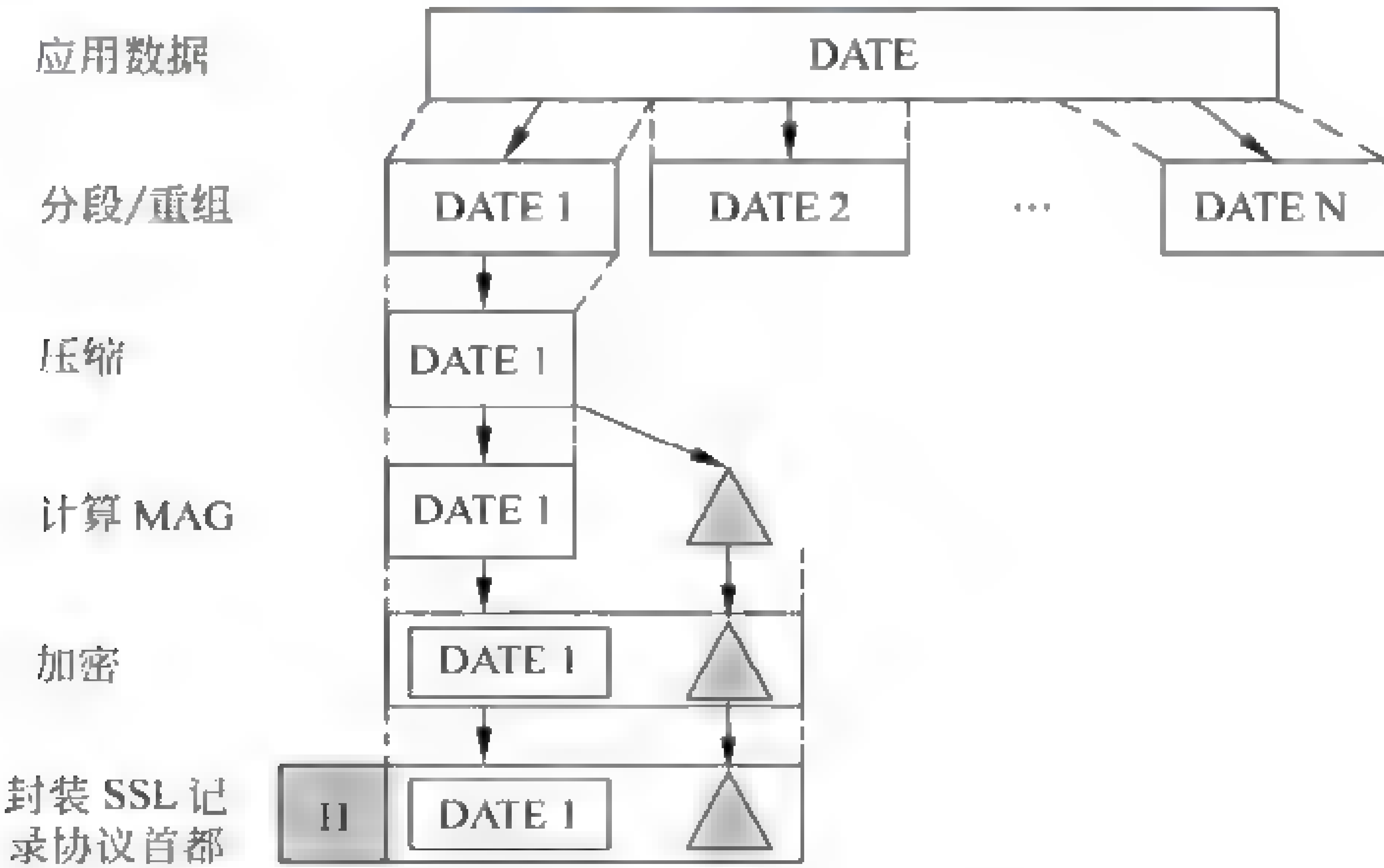


图 4-122　SSL 记录协议的操作过程

（1）分段。对应用层数据都要进行分段，使其符合规定的长度。

（2）压缩。压缩是可选的，SSL 没有指定压缩算法，压缩必须是无损的。

（3）给压缩后的数据计算消息验证码。MAC 使用下面公式进行计算：

```
Hash (MAC_write_secret+pad_2+hash (MAC_write_secret+pad_1+seq_num+
SSLCompressed.type+SSLCompressed.length+SSLCompressed.fragment))
```

其中各参数的含义如下。

- MAC write secret：为客户服务器共享的秘密。
- pad 1：为字符 0x36 重复 48 次（MD5）或 40 次（SHA）。
- pad 2：为字符 0x5c 重复 48 次（MD5）或 40 次（SHA）。
- seq_num：为消息序列号。
- Hash：为哈希算法。
- SSLCompressed.type：为处理分段的高层协议类型。
- SSLCompressed.length：为压缩分段的长度。
- SSLCompressed.fragment：为压缩分段，没有压缩时就是明文分段。

（4）使用对称加密算法给添加了 MAC 的压缩消息加密。

（5）添加 SSL 记录协议首部。

4.11.1.3 告警协议

告警协议用来为对等实体传递 SSL 的相关警告，用于标示在什么时候发生了错误或两个主机之间的会话在什么时候终止。当其他应用协议使用 SSL 时，根据当前的状态来确定。告警消息都封装成 8 位，同时进行编码、压缩和加密。

4.11.1.4 握手协议

SSL 握手协议是 SSL 中最复杂的部分。SSL 握手协议位于 SSL 记录协议层之上，用于产生会话状态的密码参数，允许服务器和客户机相互验证、协商加密和 MAC 算法及秘密密钥，用来保护在 SSL 记录中传送的数据。握手协议是在应用程序传输之前使用的。当 SSL 客户端与服务器第一次开始通信时，它们要确认协议版本的一致性，选择加密算法和认证方式，并使用公钥技术来生成共享密钥。

这个过程可以总结如下（如图 4-121 所示）。

（1）客户方向服务方发送一个 CH（Client Hello）消息，服务方以一个 SH（Server Hello）消息应答，否则通信中止。CH 和 SH 包括协议版本、会话 ID、密码配置和压缩方法等内容，此外还要交换两个随机数，记为 ClientHello.random 和 ServerHello.random。其中，密码配置表明了 SSL 客户端和 SSL 服务器都支持的某个密码组。SSL 3.0 协议规范定义了 31 种密码配置，配置主要包含三个方面的内容。

- 密钥交换方法（Key Exchange Method）。
- 数据传输加密算法（Cipher for Data Transfer）。
- 计算消息认证码的消息摘要方法（Message Digest for Creating the MAC）。

（2）若应用层需要对服务方进行认证，服务方将发送它的证书，若服务方无证书或其证书只做签名用，服务方可发送一个 SKE（Server Key Exchang）消息，以进行密钥交换。

（3）服务方向客户方请求一个与其密码配置相匹配的客户方证书。

（4）以上工作完成，服务方可发送 SHD（Server Hello Done）消息，标志着问候结束。服务器进入等待客户方响应状态。

（5）客户方在收到服务方的请求证书的消息之后，应响应一条包含证书的消息，若无证书，将响应一条无证书提示的警告。然后发送 CKE（Client Key Exchange）消息，消息内容是基于双方认可的公钥算法。

（6）若客户方发送了含签名功能的证书，则还需发送一条 DSCV（Digitally-Signed Certificate Verify）消息，以告知服务方对证书进行验证。

（7）客户方发送一条 CCS（Change Cipher Spec）消息，确认密码配置将进行更新，并更新会话的密码配置，然后用新的算法和密钥发送一条 CHF（Client HandShaking Finished）消息，表明握手结束。

（8）服务方作为回应，也发送一条 CCS（Change Cipher Spec）消息，并更新会话的密码配置，然后用新的算法和密钥发送一条 SHF（Server HandShaking Finished）消息，表明握手过程结束。至此，整个握手过程结束，客户方和服务方开始交换应用层数据。

在以上的过程中，有些消息的发送是可选的。图 4-123 表明了整个握手的流程，其中消息名称之后带“*”号的是可选的。

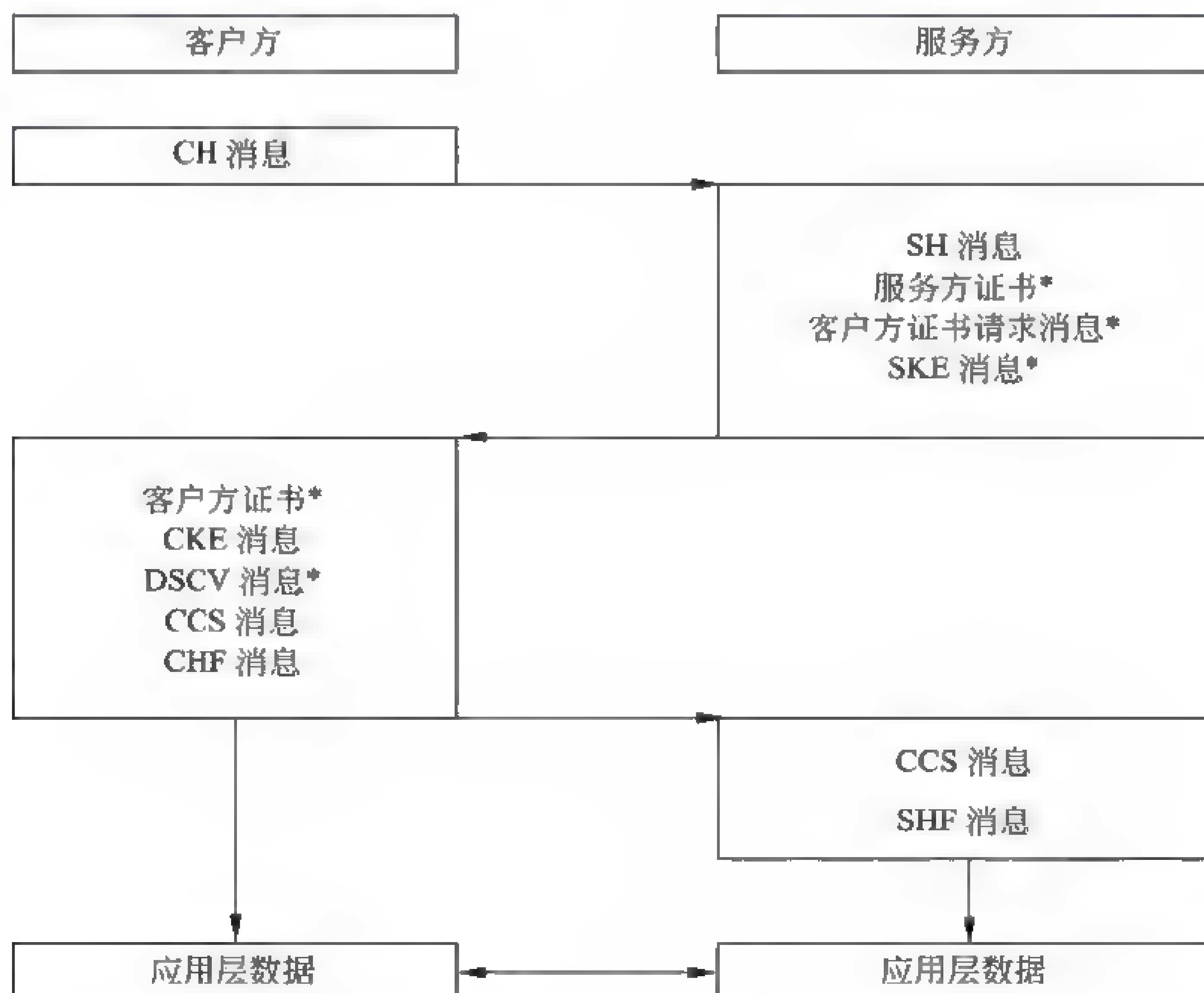


图 4-123　SSL 握手协议

4.11.2 SET 协议

4.11.2.1 SET 协议概述

1995 年，包括 MasterCard、IBM 和 Netscape 在内的联盟开始着手进行安全电子支付协议（SEPP）的开发，VISA 和微软组成的联盟开始开发安全交易技术（STT）。由于两大信用卡组织 MasterCard 和 VISA 分别支持独立的网络支付解决方案，影响了网络支付的发展。1996 年，这些公司宣布它们将联合开发一种统一的标准，叫安全电子交易（SET）。1997 年 5 月，SET 协议由 VISA 和 MasterCard 两大信用卡公司联合推出，在 Internet 支付产业中许多重要的组织，如 IBM、HP、Microsoft、Netscape、GTE 和 Verisign 等都声明支持 SET。SET 协议已获得 IETF 标准认可，已成为事实上的工业标准。SET 主要由 SET 业务描述、SET 程序员指南和 SET 协议描述三个文件组成。

SET 主要是为了解决用户、商家和银行之间通过信用卡支付的交易而设计的，以保证支付信息的机密、支付过程的完整、商户及持卡人的合法身份以及可操作性。SET 非常详细而准确地反映了交易各方之间存在的各种关系。它定义了加密信息的格式和付款支付交易过程中各方传输信息的规则。SET 提供了持卡人、商家和银行之间的认证，确保了网上交易数据的机密性、数据的完整性及交易的不可抵赖性。

4.11.2.2 SET 协议的参与者

在 SET 协议系统中，包括如下交易的参与者。

（1）持卡人（Cardholder）：在电子商务环境中，持卡人通过计算机和网络访问电子商家，购买商品。为了在电子商务环境中安全地进行支付操作，持卡人需要安装一套基于 SET 标准的软件（通常嵌入在浏览器中），并使用由发卡行发行的支付卡，而且需要从认证中心获取自己的数字签名证书。

（2）商家（Merchant）：在电子商务环境中，商家通过自己的网站向客户提供商品和服务。同时，商家必须与相关的收单行达成协议，保证可以接受信用卡的支付。而且商家也需要从认证中心获取相应的数字证书（包括签名证书和交换密钥证书）。

（3）发卡行（Issuer）：发卡行为每一个持卡人建立一个账户，并发放支付卡。一个发卡行必须保证对经过授权的交易进行付款。

（4）收单行（Acquirer）：收单行为每一个网上商家建立一个账户，且处理付款授权和付款结算等。收单行不属于安全电子商务的直接组成部分，但它是授权交易与付款结算操作的主要参与者。

（5）支付网关（Payment Gateway）：是指收单行或指定的第三方运行的一套设备。它负责处理支付卡的授权和支付。同时，它要能够同收单行的交易处理主机通信，还需要从认证中心获取相应的数字证书（包括签名证书和交换密钥证书）。

（6）品牌（Brand）：通常金融机构需要建立不同的支付卡品牌，每种支付卡品牌都有不同的规则，支付卡品牌将确定发卡行、收单行与持卡人和商家之间的关系。

（7）认证中心（Certifieate Authority）：负责颁发和撤销持卡人、商家和支付网关的数字证书。同时，它还要向商家和支付网关颁发交换密钥证书，以便在支付过程中交换会话密钥。

在实际的系统中，发卡行和收单行可以由同一家银行担当，支付网关也可由该银行来运行，这些需要根据具体的情况来决定。

4.11.2.3　SET 协议的安全机制

SET 协议同时是 PKI 框架下的一个典型实现。安全核心技术主要有公开密钥加密、数字签名、数字信封、消息摘要和数字证书等，主要应用于 B2C 模式中保障支付信息的安全性。任何一个信任 CA 的通信方，都可以通过验证对方数字证书上的 CA 数字签名来建立起与对方的信任关系，并且获得对方的公钥。为了保证 CA 所签发证书的通用性，通常证书格式遵守 ITU X.509 标准。

根据 SET 标准，对证书通过信任级联关系用分层结构进行管理。SET 定义了一套完备的证书信任链，每个证书连接一个实体的数字签名证书。沿着信任树可以到一个众所周知的信任机构，用户可以确认证书的有效性。对于所有使用 SET 的实体来说，只有唯一的根 CA。图 4-124 描述了这种信任层次。在 SET 中，用户对根节点的证书是无条件信任的，如果从证书所对应的节点出发沿着信任树逐级验证证书的数字签名，若能够到达一个已知的信任方所对应的节点或根节点，就能确认该证书是有效的。换而言之，信任关系是从根节点到树叶传播的。根密钥（RootKey）由 CA 自己签名发布，而根密钥证书由软件开发商插入他们的软件中。软件通过向 CA 发出一个初始化请求（包括证书的 Hash 值），可以确定一个根密钥的有效性。根密钥也需定期更换。为了保证根证书的真实性，根证书和下一次替换密钥的公钥的散列值一起颁发。在根证书被新的证书替代时，可通过验证证书中公钥的散列值与最近的旧证书一起颁发的散列值是否相同来对新证书的真实性进行验证。

持卡人证书、商户证书和支付网关证书分别由持卡人认证中心（CCA）、商户认证中心（MCA）和支付网关认证中心（PCA）进行颁发，而 CCA 证书、MCA 证书和 PCA 证书则由品牌认证中心（BCA）或区域性认证中心（GCA）进行颁发。BCA 的证书由根认证中心（RCA）进行颁发。

（1）持卡人证书（Cardholder CertifiCates）：相当于支付卡的电子表示，它可以由付款银行数字签名后发放。由于证书的签名私钥仅为付款银行所知，所以证书中的内容不可能被任何第三方更改。持卡人证书只有在付款银行的同意下发给持卡人。该证书同购买请求和加密后的付款指令一起发给商家，商家在验证此证书有效后，就可以认为持卡人为合法的使用者。持卡人的证书是一个数字签名证书，用于验证持卡人的数字签名，

而不能用于会话密钥的交换。任何持卡人只有在申请到数字证书之后，才能够进行电子交易。

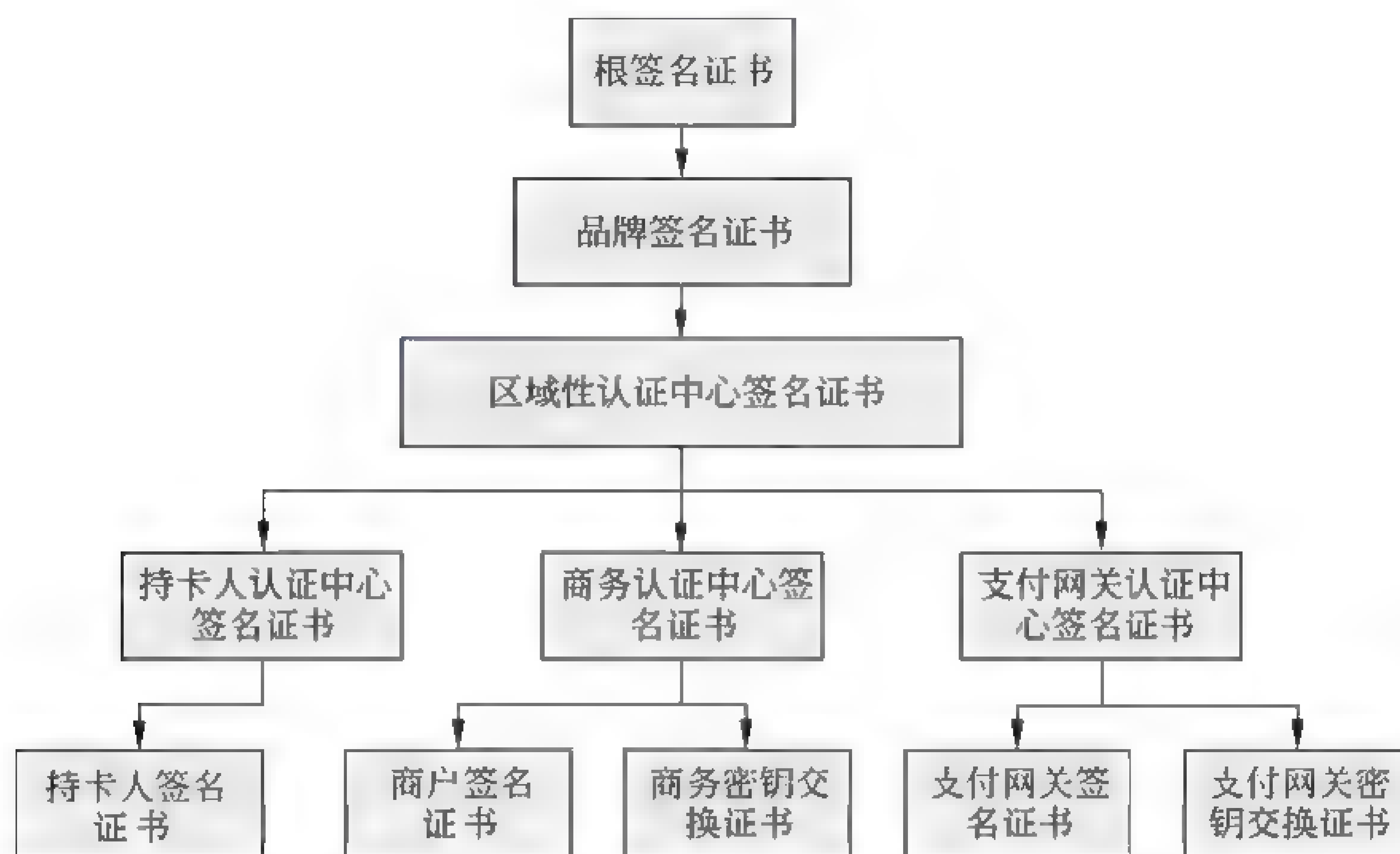


图 4-124　SET 协议中证书的层次模型

（2）商家证书（Merchant Certificates）：表示商家与收单行有联系，收单行同意商家接受付款卡支付。商家证书由收单行数字签名后颁发。商家要加入 SET 的交易至少要拥有一对证书：一个为签名证书，用来让其他用户验证商家对交易信息的数字签名；另一个为交换密钥证书，用来在交易过程中交换用于加密交易信息的会话密钥。事实上，一个商家通常拥有多对证书，以支持不同品牌的付款卡。

（3）支付网关证书（Payment Gateway Certificates）：用于商家和持卡人在进行支付处理时对支付网关进行确认以及交换会话密钥，因此一个支付网关也应该拥有两个证书：签名证书和交换密钥证书。持卡人在支付时从支付网关的交换密钥证书中得到保护他的支付卡账号及密码的公开密钥。通常支付网关证书由付款卡品牌 CA 发给收单行。

（4）收单行证书（Acquirer Certificates）：收单行必须拥有一个证书以便运行一个证书颁发机构，它接收和处理商家通过公共网络或私有网络传来的证书请求和授权信息。收单行证书由付款卡品牌 CA 发给收单行。

（5）发卡行证书（Issuer CertifiCates）：发卡行必须拥有一个证书以便运行一个证书颁发机构，它接收和处理持卡人通过公共网络或私有网络传来的证书请求和授权信息。发卡行证书由付款卡品牌 CA 发给发卡行。

SET 协议使用密码技术来保障交易的安全，主要包括散列函数、对称加密算法和非对称加密算法等。SET 中默认使用的散列函数是 SHA，对称密码算法则通常采用 DES，公钥密码算法一般采用 RSA。

在用 RSA 加密时，如果直接对明文加密，那么对密文进行分析，从而得到明文的一些位是可能的，而且这样的技术确实存在。因此，SET 在数字信封中用 RSA 加密会话密钥或是持卡人账号的时候，首先用 OAEP 算法对明文编码。OAEP 算法的作用是使消息的各位之间相互联系在一起，从而使得根据密文来求解明文的任意位的难度是相同的。

4.11.2.4　SET 协议的数据封装

SET 协议经常使用的数据封装格式包括数字信封封装和双数字签名封装以及相应的数据封装格式。

（1）持卡人账号的盲化及散列消息封装。散列函数在 SET 中除了与签名算法结合使用以及进行消息的完整性验证之外，还用来保护持卡人账号的安全。在持卡人证书中不直接包含账号信息，而是把它盲化以后放入证书中。在盲化账号时，使用散列函数和持卡人与 CCA 共享的密码值。将共享的密码值（记为 k）作为密钥，以账号、有效期等相关信息作为信息（记为 t），计算带密钥的散列值 HMAC（t，k）作为盲化的账号放入证书。因此，只有 CCA、持卡人和发卡行才能对账号进行认证。

（2）数字签名封装。SET 协议数字签名数据的封装格式使用 PKCS#10 中 SignedData 数据格式，如图 4-125 所示。

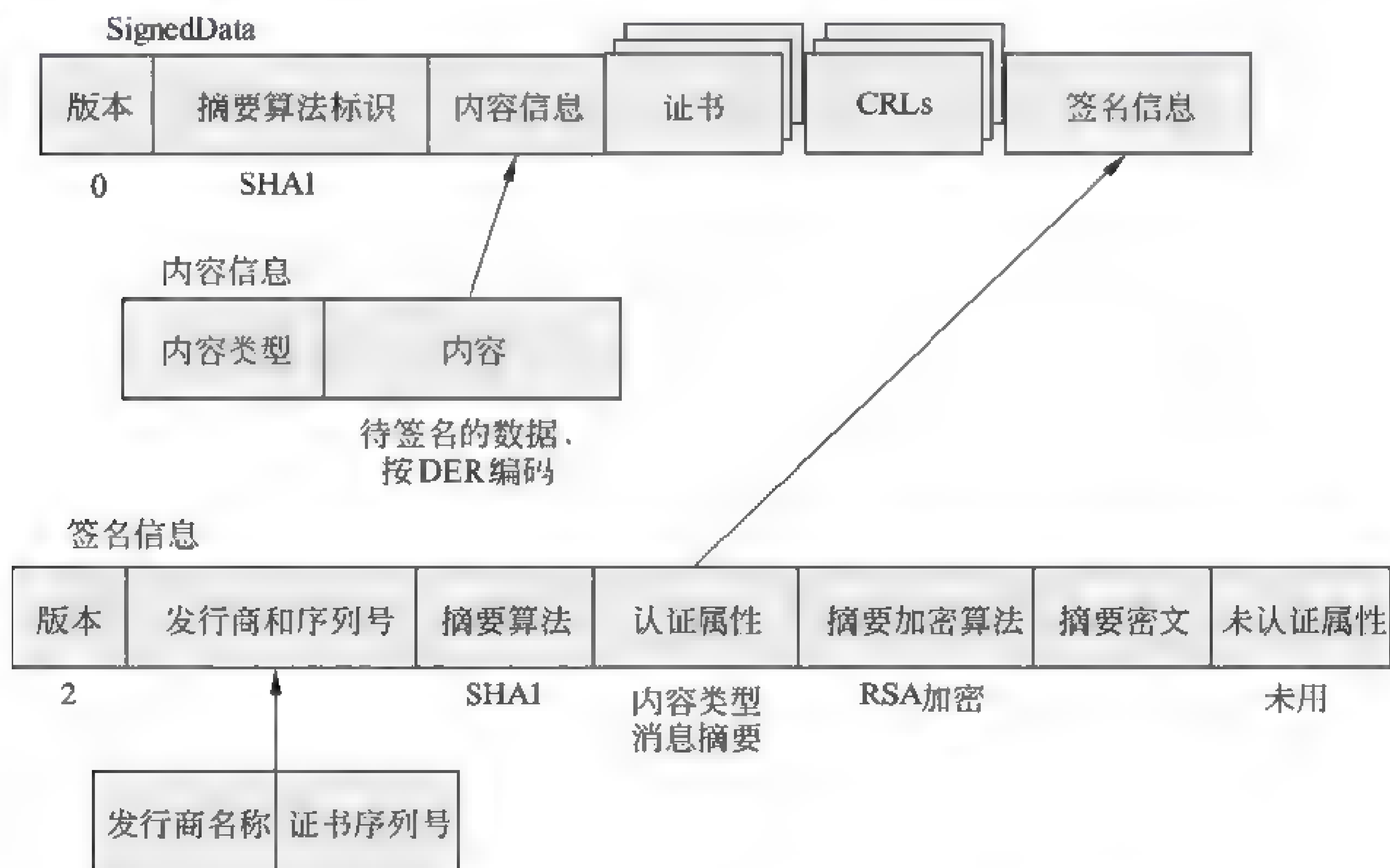


图 4-125　SignedData 数据格式

（3）数字信封（Digital Envelope）封装。在 SET 中，数字信封封装的详细格式使用了 PKCS#10 中的 EnvelopedData，如图 4-126 所示。其中，加密数据的封装格式使用了

PKCS# 10 中的 EncryptedData，如图 4-127 所示。

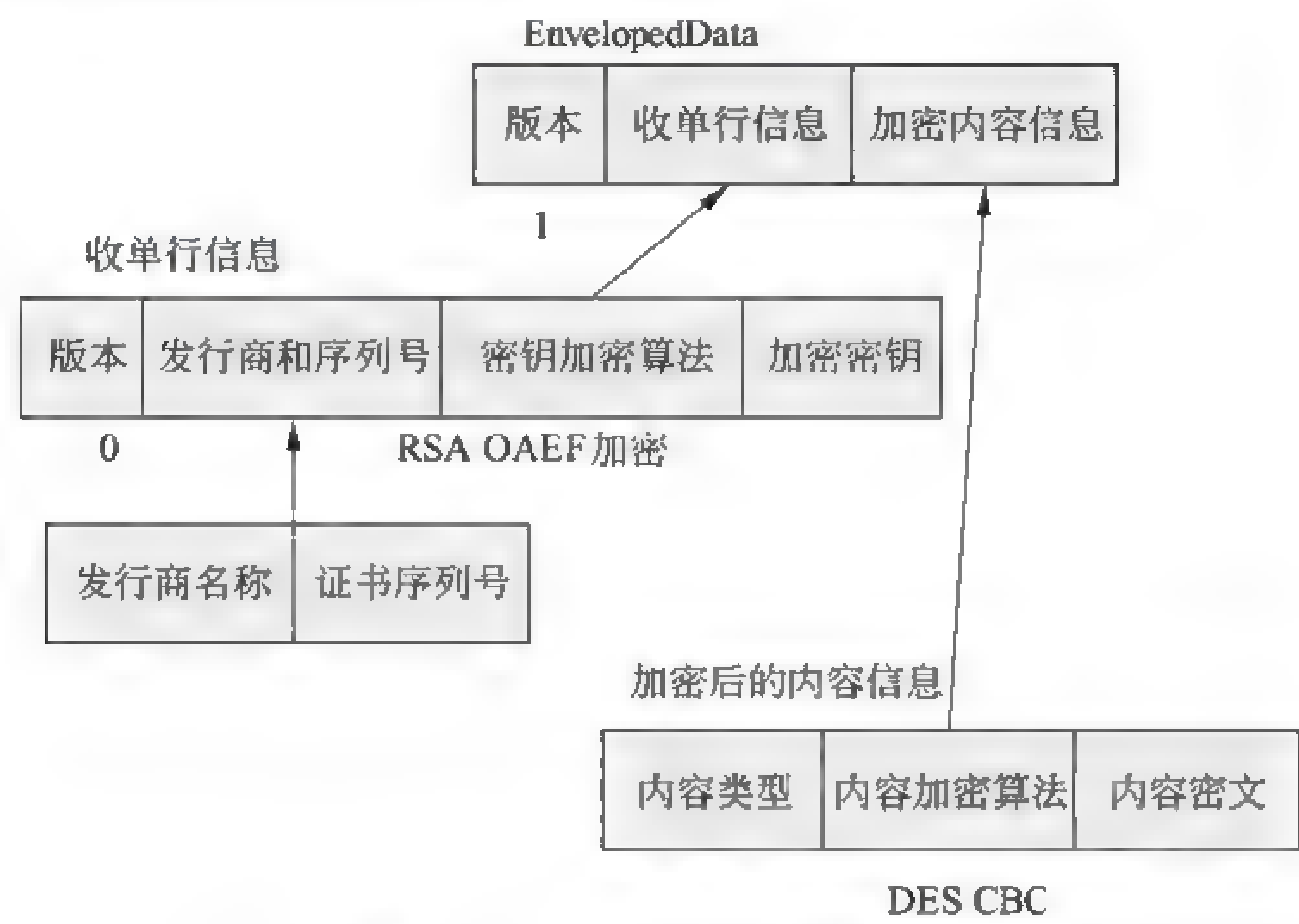


图 4-126　EnvelopedData 数据格式

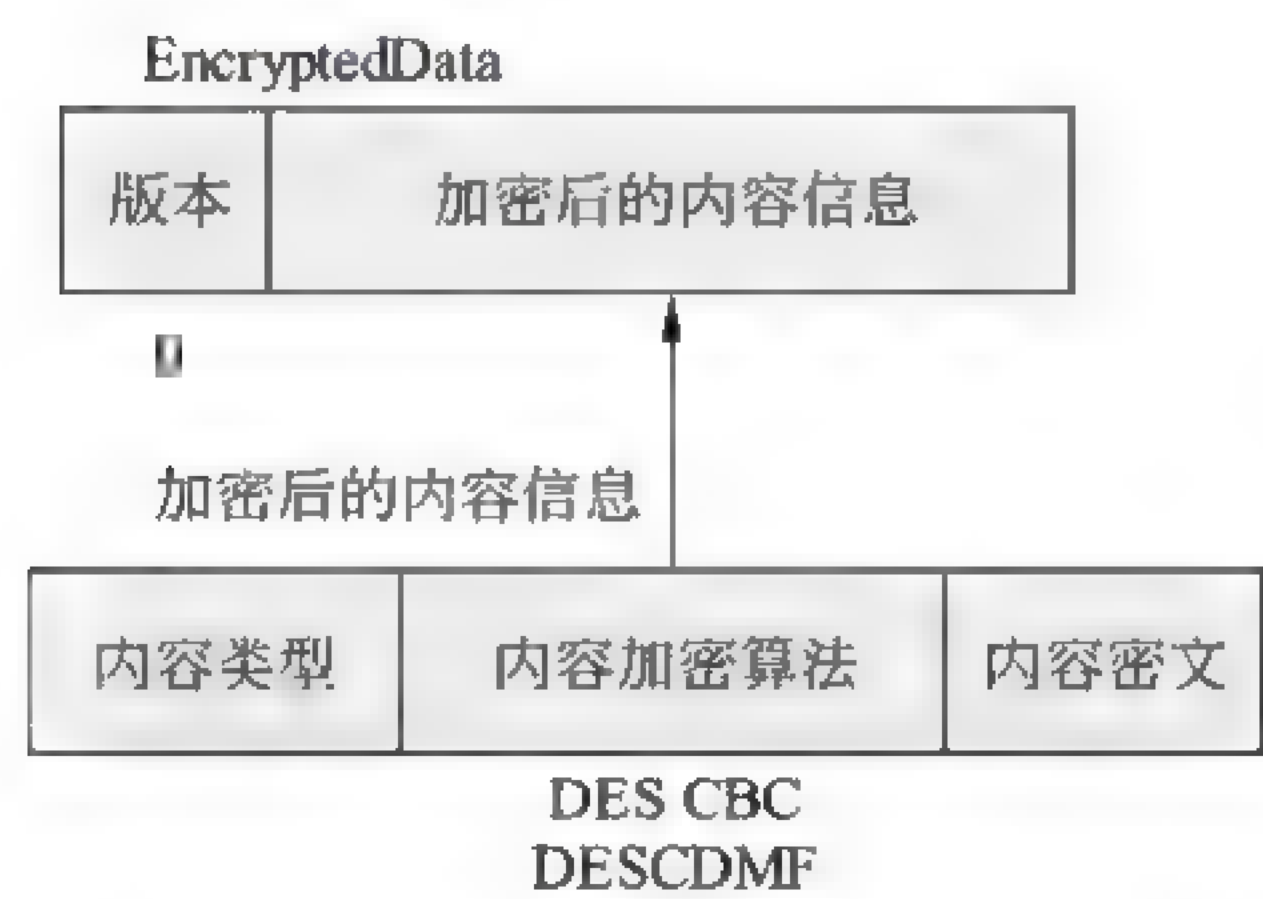


图 4-127　EncryptedData 数据格式

（4）双数字签名（Dual Signature）封装。在 SET 的交易流程中，持卡人在支付时需要对订单信息（OI）和支付信息（PI）进行双数字签名。双数字签名的作用一方面使得商家能够验证持卡人确实对 OI 和 PI 进行了签名，但只能看到 OI，而不知道 PI 的具体内容；而另一方面使得支付网关能够验证持卡人确实对 OI 和 PI 进行了签名，但只能看到 PI，而不知道 OI 的具体内容。事实上，双数字签名只是对签名的内容和数据的封装作了改动。双重数字签名的实现过程如图 4-128 所示。

① 持卡人分别计算 OI 和 PI 的消息摘要 OI digest 和 PI digest。

② 计算 OI digest | PI digest 的消息摘要 Digest，|表示位串的连接。

③ 持卡人用自己的签名私钥对 Digest 签名。

持卡人将 PI digest、OI 和双数字签名经数字信封加密后发送给商家，将 OI digest、PI 和双数字签名经数字信封加密后经由商家转发给支付网关。商家解开信封，生成订单的摘要后和账号的摘要连接起来，用持卡人证书的签名公钥即可验证签名。

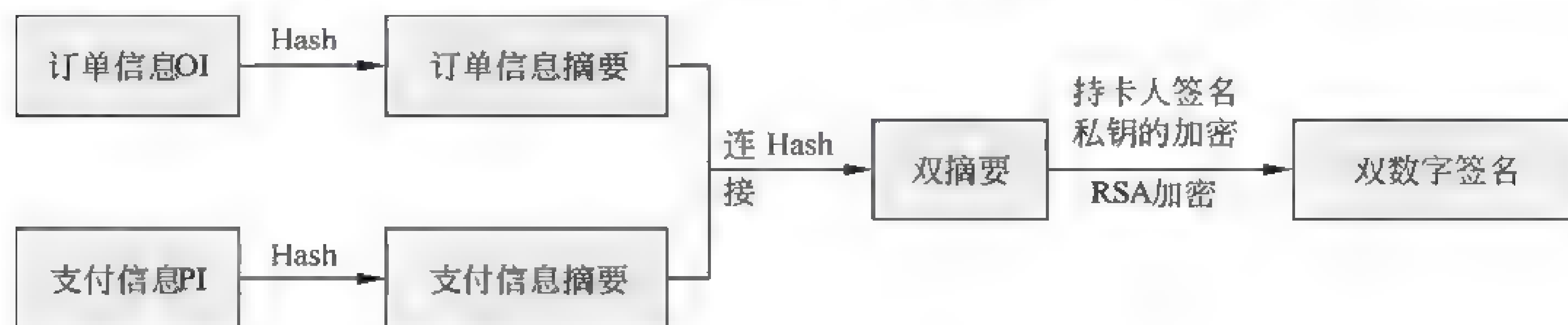


图 4-128　双数字签名

4.11.2.5　SET 协议的交易流程

SET 安全电子交易的整个过程大体可分为以下几个阶段：持卡人（C）注册、商家（M）注册、购买请求、付款授权和付款结算。

1）持卡人注册（Cardholder Registration）

持卡人 C 在实施电子交易之前必须先向其金融机构（发卡行）注册登记，以便得到一个签名证书。在这个过程中，C 为了保证信息的机密性，需要使用 CCA 的交换密钥的公钥。它是从 CCA 的交换密钥证书（在初始响应中由 CCA 发送）中得到的。图 4-129 描述了持卡人通过 SET 协议申请证书的信息流程。

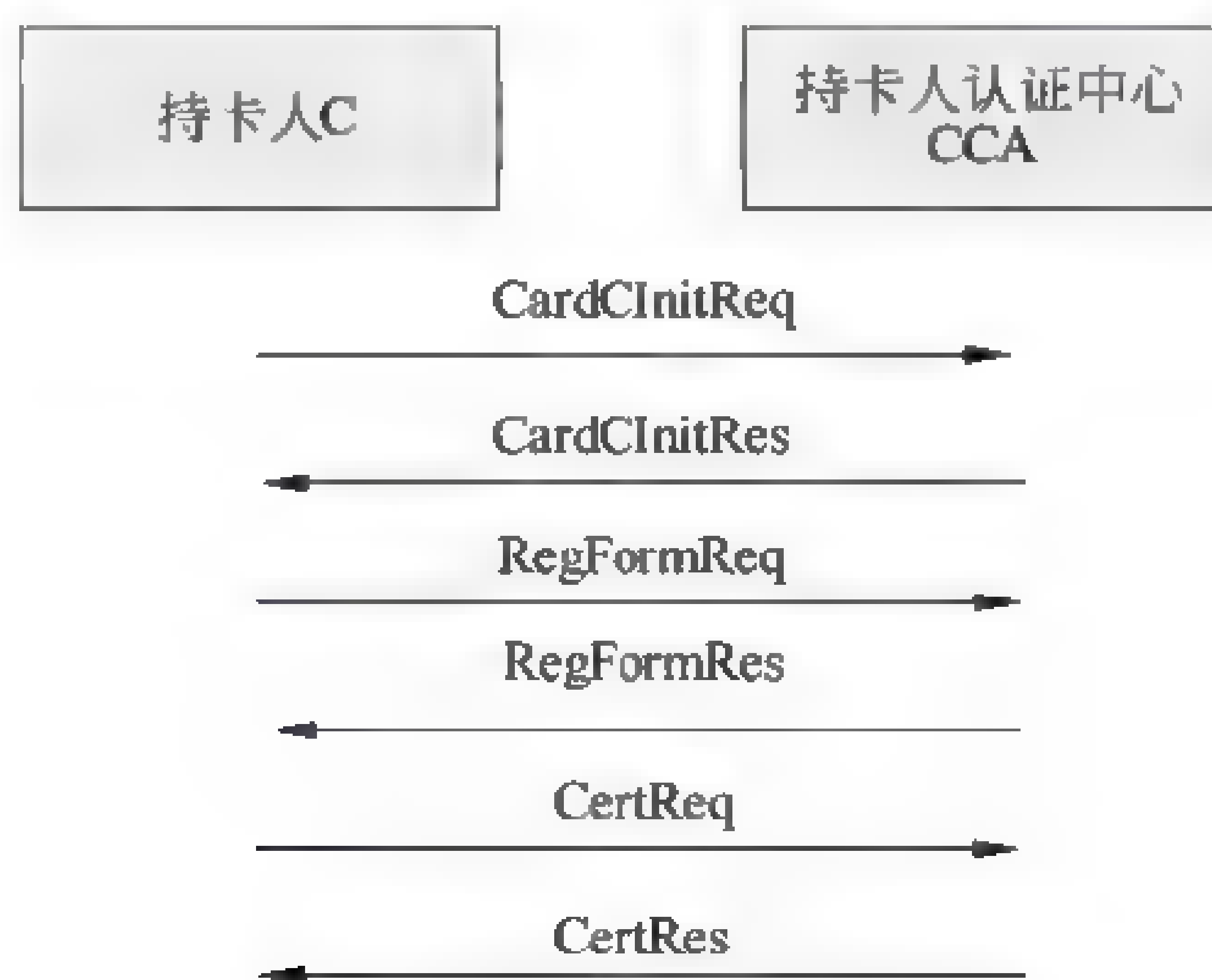


图 4-129　持卡人申请证书的流程

注册的具体步骤如下。

（1）C 向 CCA 发送初始请求 CardCInitReq。

（2）CCA 接到初始请求，生成初始响应 CardCInitRes，并对初始响应进行数字签名；CCA 把 CardCInitRes 连同证书一起发给 C。

（3）接到初始响应，并验证 CCA 的证书；接着验证 CCA 对响应的数字签名。

（4）C 输入账号，生成注册表请求 RegFormReq；C 随机生成对称密钥 K_1，用 K_1 对注册表请求消息加密，K_1 与账号一起用 CCA 的交换密钥的公钥加密；C 发送加密后的 RegFormReq 给 CCA。

（5）CCA 用交换密钥的私钥解密 K_1 和账号，用 K_1 解密加密的 RegFormReq。

（6）CCA 选择合适的注册表，生成注册表响应 RegFormRes，并对其进行数字签名；CCA 发送加密的 RegFormRes 及 CCA 的证书给 C。

（7）C 接收 RegFormRes 并验证 CCA 的证书；接着验证 CCA 对注册表的数字签名；C 产生一对公开/秘密密钥 SignatureKeyPair 和一个秘密的用于注册账号的随机数 R_1；C 填写注册表并生成证书请求 CertReq。

（8）C 生成由 CertReq、C 的公开密钥和新生成的对称密钥 K_2 组成的消息，并签名；C 将此消息用密钥 K_3 加密，K_3、R_1 与账号一起用 CCA 的交换密钥的公钥加密；C 发送这个消息（包括加密的账号和 R_1 等）给 CCA。

（9）CCA 用交换密钥的私钥解密 K_3、随机数 R_1 和账号，用 K_3 解密加密后的证书请求；CCA 验证 C 的数字签名，用账户信息和注册表信息对 C 进行必要的验证（SET 中没有具体规定）；根据验证结果，CCA 生成随机数 R_2，将 R_2、R_1、C 的账号、有效期等信息的散列值包含在证书中，并签名，生成证书。

（10）CCA 生成证书应答 CertRes（包含有加密的 R_2）并签名；CCA 将 CertRes 用 K_2 加密后发送给 C。

（11）C 验证 CCA 的证书并用 K_2 解密消息 CertRes；C 验证 CCA 对证书的数字签名后保留证书以及 CCA 产生的秘密随机数 R_2。

在持卡人注册过程中，C 的证书不直接包含 C 的账号，而是包含相关信息的散列值。因此，仅有证书提供的信息是不可能推知出账号信息的，这样就保护了持卡人的敏感信息；此外，C 没有交换密钥证书，会话密钥总是由 C 产生并通过 CCA 的交换密钥的公钥加密传递。

2）商家注册（Merehant Registration）

商家 M 在进行电子交易之前，必须先向其金融机构（收单行）注册登记，以便得到签名证书和交换密钥证书。而支付网关的证书获取过程同商家的一样。图 4-130 描述了商家（或支付网关）通过 SET 协议申请证书的流程。

注册的具体步骤如下。

（1）M 发送初始请求 Me-AqCInitReq 给 MCA。

（2）MCA 接收到消息 Me-AqCInitReq，选择合适的注册表，生成初始响应 Me-AqCInitRes，并对其进行数字签名；MCA 发送 Me-AqCInitRes 及 MCA 的证书给 M。



图 4-130 商家（或支付网关）申请证书的流程

（3）M 验证 MCA 对消息的数字签名，并产生两对公开/秘密密钥：Key-eXChange Pair 和 SignatureKeyPair；M 填写注册表并生成证书请求 CertReq；M 生成请求和两个公开密钥构成的消息并签名；M 将消息用随机生成的密钥 K_1 加密，K_1 及 M 的账户信息用 MCA 的交换密钥的公钥加密；M 把消息发送给 MCA。

（4）MCA 收到消息，用交换密钥的私钥解密 K_1 和 M 的账户信息，并用 K_1 解密消息；M 以验证 M 的数字签名，使用 M 的有关信息证实 CertReq；根据验证 MCA 生成 M 的证书并对其签名；M 以生成证书响应 CertRes 并签名；MCA 发送证书和 CertRes 给 M。

（5）M 验证 CertRes 的签名，接着验证 M 以颁发的证书的数字签名，并保留证书。

3）购买请求（purehase Request）

购物请求的具体步骤如下。

（1）C 通过一定的方式挑选商品。选完后，C 发送初始请求给 M。

（2）M 接收初始请求，并生成初始响应，对其进行数字签名；M 把初始响应、M 和 PG 的证书发送给 C。

（3）C 接收到初始响应，并验证所有的证书；C 验证 M 对初始响应的数字签名；C 生成订单信息 OI 和付款指令信息 PI，并对 OI 和 PI 进行双数字签名；C 用随机生成的对称密钥 K_1 对 PI 加密，K_1 和 C 的账户信息用 PG 的交换密钥的公钥加密；C 发送 OI 及加密的 PI 给 M。

（4）M 验证 C 的证书及 C 的双数字签名；M 处理购买请求，生成购买响应（包括 M 的证书）并对其签名，发送给 C。

（5）若交易已经授权，则 M 履行合同。

（6）C 接收购买响应后，验证 M 的证书，进一步验证 M 对购买响应的数字签名；C 保留购买响应。

在购买请求中，双数字签名的作用是使商家可以验证 OI 和 PI 是由持卡人进行签名的，但商家却不能够看到 PI 的具体内容。而对于支付网关而言，它也能够验证 OI 和 PI 是由持卡人进行签名的，但它不能够看见 OI 的具体内容。使用双数字签名的好处是不仅能够对消息源、消息完整性进行认证，而且使信息得到了最大程度的保护。

4）付款授权（payment Authorization）

在购买请求的过程中，M 还要在发送购买响应之前完成付款授权，其具体步骤如下。

（1）M 生成授权请求，并对其进行签名；M 将授权请求用随机生成的对称密钥 K_2 加密，K2 则用 PG 的交换密钥的公钥加密；M 将加密后的信息和 M 的证书一起发送给 PG。

（2）验证 M 的证书，用自己的交换密钥私钥解密 K_2，用 K_2 解密授权请求；PG 验证 M 对授权请求的签名；接着，验证 C 的证书，用自己的交换密钥私钥解密 K_1，用 K_1 解密付款指令 PI；PG 验证 C 的双数字签名，验证 M 的授权请求与 C 的付款指令的一致性；PG 将授权请求通过金融网络发送给 C 的金融机构。

（3）PG 生成授权响应并对其进行数字签名，用 K_3 对授权响应加密，而 K_3 用 M 的交换密钥公钥加密；PG 生成结算标记并签名，并用 K_4 加密，K_4 及 C 的账户信息用 PG 的交换密钥公钥加密；PG 将加密的响应及自己的证书发送给 M。

（4）M 验证 PG 的证书，用自己的交换密钥私钥解密 K_3，用 K_3 解密响应消息；M 验证 PG 对授权响应的数字签名，M 保留结算标记供以后使用，并完成购买请求。

5）付款结算（Payment Capture）

M 在履行合同之后要求结算付款。在付款授权和付款结算之间经常有较长的时间间隔。具体的付款结算步骤如下。

（1）M 生成结算请求，并把自己的证书加入结算请求中，进行数字签名；M 将结算请求用 K_5 加密，K_5 用 PG 的交换密钥公钥加密，发送加密的结算请求及在授权过程中保留的加密了的结算标记给 PG。

（2）PG 首先验证 M 的证书，用自己的交换密钥私钥解密 K_5，用 K_5 解密结算请求；PG 验证 M 对结算请求的数字签名，用自己的交换密钥私钥解密 K_4，用 K_4 解密结算标记，确认结算请求与结算标记的一致性。

（3）PG 生成结算响应消息（包括 PG 的证书），并签名；PG 将结算响应用 K_6 加密，K_6 用 M 的交换密钥公钥加密，最后发送给 M。

（4）M 验证 PG 的证书，用自己的交换密钥私钥解密 K_6，用 K_6 解密结算响应；M 验证 PG 对结算响应的签名，保留结算响应以便用来从收单行提款。

4.11.3 HTTPS

4.11.3.1 HTTPS 的概念

HTTPS（Hypertext Transfer Protocol over Secure Socket Layer，基于 SSL 协议的 HTTP）是一个安全通信通道，用于在客户计算机和服务器之间交换信息。它使用安全套接字层进行信息交换，所有的数据在传输过程中都是加密的。HTTPS 最初的研发由网景公司进行，提供了身份验证与加密通信方法，现在它被广泛用于全球信息网上安全敏感的通信，

例如交易支付方面。

严格来说，HTTPS 不是一个单独的协议，而是两个协议的结合，即在加密的安全套接层或传输层安全（TLS）上进行普通的 HTTP 交互传输。这种方式提供了一种免于窃听者或中间人攻击的合理保护。

要使一个网络服务器接受 HTTPS 连接，管理员必须为服务器生成一个电子证书。在基于 UNIX 的服务器上，这些证书可以通过一些工具，诸如 OpenSSL 的 ssl-ca 或 SUSE 的 gensslcert 来产生。

当使用 SSL/TLS（通常使用 https：// URL）向站点进行 HTTP 请求时，服务器将向客户机发送一个证书。客户机使用已安装的公共证书验证服务器的身份，然后检查 IP 名称（机器名）与客户机连接的机器是否匹配。客户机生成一些可以用来生成对话的私钥（称为会话密钥）的随机信息，然后用服务器的公钥对它加密并将它发送到服务器。服务器用自己的私钥解密消息，然后用该随机信息派生出和客户机一样的私有会话密钥。通常在这个阶段使用 RSA 公钥算法。然后，客户机和服务器使用私有会话密钥和私钥算法（通常是 RC4）进行通信。使用另一个密钥的消息认证码来确保消息的完整性。

在 RFC 2818 中，描述了如何将 TLS 应用于 Internet 上的安全的 HTTP 连接。

要注意的是，HTTPS 不同于 EIT 开发的 SHTTP，SHTTP（Secure HyperText Transfer Protocal，安全超文本转换协议）是一个 https URI scheme 的可选方案，也是为因特网的 HTTP 加密通信而设计的。S-HTTP 定义于 RFC 2660。

4.11.3.2　HTTPS 的初始化连接

作为 HTTP 客户的代理，同时也作为 TLS 的客户。在 HTTPS 初始化连接时，HTTP 客户代理向服务器的适当端口发起一个连接，然后发送 TLS ClientHello 来开始 TLS 握手。当 TLS 握手完成，客户可以初始化第一个 HTTP 请求。所有的 HTTP 数据必须作为 TLS 的“应用数据”发送。当然，正常的 HTTP 行为，如保持连接等，和 HTTP 是一样的。

4.11.3.3　HTTPS 的关闭连接

TLS 提供了安全关闭连接的机制。当收到一个有效的关闭警告时，这个连接上不再接收任何数据。TLS 的实现在关闭连接之前发起交换关闭请求。TLS 实现可能在发送关闭请求后，不等待对方发送关闭请求即关闭该连接，产生一个“不完全的关闭”。

一个未成熟请求并不质疑数据已被安全地接收，而仅意味着接下来数据可能被截掉。由于 TLS 并不知道 HTTP 的请求/响应边界，为了解数据截断是发生在消息内还是在消息之间，有必要检查 HTTP 数据本身（即 Content-Length 头）。

1）客户行为

由于 HTTP 使用连接关闭表示服务器数据的终止，客户端实现上对任何未成熟的关闭要作为错误对待，对收到的数据认为有可能被截断。在某些情况下，HTTP 协议允许

客户知道截断是否发生，这样如果客户收到了完整的应答，则在遵循“严出松入[RFC 1958]”的原则下可容忍这类错误，数据截断经常不体现在 HTTP 协议数据中。有如下两种情况特别值得注意。

（1）一个无 Content-Length 头的 HTTP 响应。在这种情况下，数据长度由连接关闭请求通知，我们无法区分由服务器产生的未成熟关闭请求及由网络攻击者伪造的关闭请求。

（2）一个带有有效 Content-Length 头的 HTTP 响应在所有数据被读取完之前关闭。由于 TLS 并不提供面向文档的保护，所以无法知道是服务器对 Content-Length 计算错误还是攻击者已截断连接。

以上规则有一个例外。当客户遇到一个未成熟关闭时，客户把所有已接收到的数据同 Content-Length 头指定的一样多的请求视为已完成。

客户检测到一个未完成关闭时应予以有序恢复，它可能恢复一个以这种方式关闭的 TLS 对话。客户在关闭连接前必须发送关闭警告。未准备接收任何数据的客户可能选择不等待服务器的关闭警告而直接关闭连接，这样在服务器端产生一个不完全的关闭。

2）服务器行为

RFC 2616 允许 HTTP 客户在任何时候关闭连接，并要求服务器有序地恢复它。特别是服务器应准备接收来自客户的不完全关闭，因为客户往往能够判断服务器数据的结束。服务器应乐于恢复以这种方式关闭的 TLS 对话。

在实现上，在不使用永久连接的 HTTP 实现中，服务器一般期望能通过关闭连接通知数据的结束。但是，当 Content-Length 被使用时，客户可能早已发送了关闭警告并断开了连接。

服务器必须在关闭连接前试图发起同客户交换关闭警告。服务器可能在发送关闭警告后关闭连接，从而形成了客户端的不完全关闭。

4.11.3.4 HTTPS 的端口和 URI 格式

HTTPS 是一个 URI scheme（抽象标识符体系），用于安全的 HTTP 数据传输，句法类同 http：体系。https：URL 表明它使用了 HTTP，但 HTTPS 存在不同于 HTTP 的默认端口及一个加密/身份验证层（在 HTTP 与 TCP 之间）。https：URL 连接可以指定 TCP 端口，否则使用默认的 443 端口（普通 HTTP 连接一般使用 80 端口）。

HTTP 服务器期望最先从客户收到的数据是 Request-Line production，TLS 服务器期望最先收到的数据是 ClientHello。因此，一般做法是在一个单独的端口上运行 HTTP/TLS，以区分是在使用哪种协议。当在 TCP/IP 连接上运行 HTTP/TLS 时，默认端口是 443。这并不排除 HTTP/TLS 运行在其他传输上。TLS 只假设有可靠的、面向连接的数据流。

HTTP/TLS 和 HTTP 的 URI 不同，使用协议描述符 https 而不是 http。使用 HTTP/TLS 的一个 URI 例子是：

https：//www.example.com/~smith/home.html

4.11.3.5　端标识

1）服务器身份

通常，解析一个 URI 产生 HTTP/TLS 请求，结果客户得到服务器的主机名。若主机名可用，为防止有人在中间攻击，客户必须把它同服务器证书信息中的服务器的身份号比较检查。

若客户有相关服务器标志的外部信息，主机名检查可以忽略（例如，客户可能连接到一个主机名和 IP 地址都是动态的服务器上，但客户了解服务器的证书信息）。在这种情况下，为防止有人攻击，尽可能缩小可接受证书的范围就很重要。在特殊情况下，客户简单地忽略服务器的身份是可以的，但必须意识到连接对攻击是完全敞开的。

若 dNSName 类型的 subjectAltName 扩展存在，则必须被用作身份标识。否则，在证书的 Subject 字段中必须使用 Common Name 字段。虽然使用 Common Name 是通常的做法，但不被推荐，而 Certification Authorities 被推荐使用 dNSName。

使用[RFC 2459]中的匹配规则进行匹配。若在证书中给定类型的身份标识超过一个（也就是超过一个 dNSName 和集合中的相匹配），名字可以包括通配符*表示和单个域名或其中的一段相匹配。例如，*.a.com 和 foo.a.com 匹配但和 bar.foo.a.com 不匹配，f*.com 和 foo.com 匹配但和 bar.com 不匹配。

在某些情况下，URI 定义的不是主机名而是 IP 地址。在这种情况下，证书中必须有 iPAddress subjectAltName 字段且必须精确匹配在 URI 中的 IP 地址。

若主机名和证书中的标识不相符，面向用户的客户端必须或者通知用户（客户端可以给用户机会来继续连接）或终止连接并报证书错。自动客户端必须将错误记录在适当的审计日志中（若有）并应该终止连接（带一证书错）。自动客户端可以提供选项禁止这种检查，但必须提供选项使能它。

注意，在很多情况下 URI 本身是从不可信任的源得到的。以上描述的检查并未提供对危害源的攻击的保护。例如，若 URI 是从一个未采用 HTTP/TLS 的 HTML 页面得到的，某个人可能已在中间替换了 URI。为防止这种攻击，用户应仔细检查服务器提供的证书是否是期望的。

2）客户标识

典型情况下，服务器并不知道客户的标识是什么也就无法检查（除非有合适的 CA 证书）。若服务器知道（通常是在 HTTP 和 TLS 之外的源得到的），它应该像上面描述的那样检查。

4.12　桌面安全解决方案

桌面系统通常是指个人使用的 PC、网络上的终端。随着网络化程度的提高，特别是

因特网应用的普及，桌面系统接入网络已经非常普遍。在开放互联的网络环境中进行办公事务、电子商务以及休闲娱乐等网络活动的同时，往往容易受到病毒的侵袭、黑客的攻击，而且病毒的传播途径和黑客的攻击手段更富多样化，行为也更隐蔽。如何保护桌面系统的安全，做到能抵御恶意攻击和病毒侵袭，保证信息在存储和传输过程中不被窃取、篡改，使得重要信息个人专用，已经成为大家越来越关注的问题。桌面安全防护几乎涉及到信息安全的各种技术，如用户安全认证网络访问控制、信息存储加密、电子邮件安全以及安全审计等。随着信息网络的迅速发展，在当今的信息时代，信息技术已经彻底改变了我们的生活和工作方式，也改变了现行企事业单位的管理模式。作为信息的管理部门，必须考虑当前技术的发展给我们的工作所带来的利益和威胁。如何利用信息网络进行安全的通信，同时保护计算机自身信息的安全性，成为当前网络安全和信息安全迫在眉睫的问题。针对日益严重的内部信息泄露问题，FBI 对 484 家公司调查显示：面对来自于公司内部的安全威胁，85%的安全损失是由企业内部原因造成的。对于很多国内企业来说，这可能有点耸人听闻。但是，他们肯定遇到过类似的事情，由于某一位员工误操作造成公司服务器上重要文档丢失；由于没有定义每位员工在系统内的访问权限，使本该由一定级别的人员才能掌握的业务秘密泄露给竞争对手。对于这些来自公司内部的安全问题，不是靠单纯安装杀毒软件或防火墙就能解决的。目前，90%以上的终端用户使用的是 Windows 2000/XP 或以上的操作系统，而这几种系统的安全漏洞又非常多，微软公司会通过定期发布安全补丁的方式来弥补这些漏洞，但由于端终用户缺乏相关知识，导致补丁安装的不完全、不及时，这就会严重影响终端计算机的安全，从而导致更严重的整个内网安全问题。

目前市场上的网络管理产品主要分为两类：一种是以资产管理功能为主的桌面管理软件，传统的桌面管理软件主要是以解决桌面计算机资产管理困难为出发点的，目前这些产品的厂商也正在逐步往产品中增加安全管理的功能；二是以安全管理为主的桌面管理软件，目前市场上新出现的产品绝大多数都是以安全管理为主的，但是多数的产品市场应用情况都不十分理想。桌面安全软件大致可以分为以下几种类型：防病毒为主的桌面安全软件，这类软件基本上专注于对抗基于 Windows 平台的病毒，现在也提供对某些类型文件的恶意代码扫描功能。个人防火墙主要是从网络的角度来保护计算机免受侵犯，主要功能是屏蔽大部分可能被攻击的网络服务。VPN 技术主要是在客户端和服务器之间建立一条安全的隧道，保证客户端和服务器之间的通信不被监听。增强操作系统主要是针对 Windows 操作系统利用某些未公开 API 来提升 Windows 操作系统的安全性，限制操作（这些工具主要用于网吧或者限制儿童使用计算机）。硬件设备利用硬件设备提供具体的安全功能，如利用 USB-key、IC 卡等实现对桌面系统的控制，控制系统的可使用性。生物特征利用指纹、虹膜和面容等生物特征作为系统登录的凭据以增强系统的安全性。利用公钥技术实现强有力的身份认证、数据加密保护、数据传输和数字签名是近几年兴起的安全技术。

桌面管理系统存在的主要问题是缺乏网络准入控制功能，无法防止外来人员将计算机接入网络，更难以防范本单位员工将外来计算机接入单位网络，难以在大型网络系统中快速发现新接入的计算机，由于发现困难进而导致管理上的困难。难以发现安装了个人防火墙的桌面计算机，由于计算机安装个人防火墙，不能通过网络 PING 通，因此很难被管理服务器发现。个人计算机如果把安装在其上面的代理卸载，管理服务器很难发现这种行为。很少有产品可以提供依据 IP 地址、MAC 地址和主机名等信息对计算机进行快速定位的功能，由于桌面计算机数量多，管理维护中经常需要解决这个问题，因此这项功能很重要。无法控制不让外来非法计算机或者不符合管理规定的计算机接入单位内部网络，目前只有少部分高端厂商的产品通过网络准入控制技术解决了这个问题。

大中型企事业单位、政府办公网络，桌面计算机数量众多，管理难度很大。计算机感染病毒、被安装木马（像目前最严重的灰鸽子），有些不明程序不断抢占 IP 地址造成其他机器无法正常工作，还有部分员工使用 BT、电驴下载工具等现象时有发生。由于难以发现有问题的计算机，难以对这些危险计算机进行定位，一旦问题发生，往往故障排查时间非常长。如果同时有多台计算机感染网络病毒或者进行非法操作，非常容易导致网络阻塞，从而致使其他正常网络业务无法使用。由于缺乏技术和管理手段，许多管理规定也难以执行。例如，在个人使用的计算机内安装 BT 下载软件，安装网络游戏软件，私自更改计算机的安全设置，将外部的计算机接入单位的内部网络等行为。这些行为违反了单位的管理规定，也影响了计算机网络的安全性，如果情况更严重，可能会导致网络瘫痪。尤其是没有相关的技术与管理手段，企业许多管理规定也难以执行。例如，上班时间不准聊 QQ，不准安装 BT 和电驴等下载工具，不准玩网络游戏，不准私自修改计算机安全设置，不准通过 IE 代理私自浏览与工作无关的网站，需要设置操作系统密码，必须安装防病毒软件并更新到最新病毒库等。这些行为违反了单位的信息化管理规定，也极大地影响了企业内部网络的安全性。

以往提起信息安全，人们更多地把注意力集中在防火墙、防病毒、IDS（入侵检测）、网络互联设备即对交换机、集线器和路由器等的管理上，却忽略了对网络环境中的计算单元——服务器、台式机乃至便携机的管理。正确、全面地认识终端桌面管理的发展趋势和技术特点，是 IT 研发厂商面临的发展抉择，同时也是企、事业 IT 管理人员和高层决策人员在进行终端桌面安全防护部署时必须考虑的议题。终端桌面安全管理技术的兴起是伴随着网络管理事务密集度的增加，作为网络管理技术的边缘产物而衍生的，它同传统安全防御体系的缺陷相关联，是传统网络安全防范体系的补充，也是未来网络安全防范体系重要的组成部分。因此，终端桌面安全管理技术无论在现在还是未来都应当归入基础网络安全产品体系之列。近两年的安全防御调查也表明，政府、企业单位中超过 80%的管理和安全问题来自终端，计算机终端广泛涉及每个用户，由于其分散性、不被重视、安全手段缺乏的特点，已成为信息安全体系的薄弱环节。因此，网络安全呈现出了新的发展趋势，安全战场已经逐步由核心与主干的防护，转向网络边缘的每一个终端。

建立桌面计算机安全管理系统的意义在于解决大批量的计算机安全管理问题。具体来说，这些问题包括加强桌面计算机的安全性，如通过批量设置计算机的安全保护措施提高桌面计算机的安全性，及时更新桌面计算机的安全补丁，减少被攻击的可能；实现动态安全评估，实时评估计算机的安全状态及其是否符合管理规定，如评估计算机的网络流量是否异常、计算机是否做了非法操作（拨号上网、安装游戏软件等）及计算机的安全设置是否合理等；批量管理设置计算机，如进行批量的软件安装、批量的安全设置等；防止外来计算机非法接入，避免网络安全遭受破坏或者信息泄密；确保本单位的计算机使用制度得到落实，如禁止拨号上网、禁止使用外部邮箱、禁止访问非法网站、禁止将单位机密文件复制及发送到外部等；出现安全问题后，可以对有问题的 IP/MAC/主机名等进行快速的定位；实现计算机的资产管理和控制。

4.12.1 终端智能登录

Windows 终端能够与多用户的 Windows 2000/XP 系统一起构成一套 Thin-Client/Server 体系。Windows 2000/XP 提供的终端服务功能，允许多个用户连到同一台服务器，每一个用户使用终端，与独立使用 PC 一样没有任何区别，相互之间互不影响。其内在的原理与传统终端一样，终端登录到服务器上，所有的软件在服务器上运行，终端仅仅是作为一个输入输出设备而已。与传统终端所不同的是，传统终端是字符界面，Windows 终端是 Windows 界面；在传统终端上运行的程序是 UNIX 下的应用程序，Windows 终端的应用程序是 DOS、Windows 95/98/2000/XP；传统终端的通信协议是简单的 RS-232 串口通信协议，而 Windows 终端是基于 TCP/IP 之上的 ICA/RDP 网络通信协议；传统终端的通信硬件接口是 RS-232 串口，Windows 终端既可以支持 RS-232 串口协议，也可以通过内置的网卡连接网络。

Windows 终端可以有效地解决网络管理同应用需要之间的矛盾。一方面，Windows 终端是 Windows 2000/XP 的标准端末设备，几乎所有的 DOS、Windows 下的应用程序都可以不加任何修改地继承使用；另一方面，使用者无须对硬件设备有什么了解也可以很好地使用。同时，做为一种高集成的电子产品，Windows 终端的零维护和可靠性也是 PC 所无法比拟的。Windows 终端以最新的网络技术为基础，使通过网络连接到服务器的 Windows 终端能够全面地实现个人计算机的功能，其带来的好处是显而易见的。

（1）组网模式灵活多样，既可以在本地局域网络环境使用，也可以在远程广域网模式下使用，既可以当作 Windows 终端来用，也可以当作 UNIX 终端使用，还可以在 IBM 的 AS/400 模式下当作 IBM 的同步仿真终端使用。如果用户愿意，在没有服务器的情况下，也可以把它当作浏览器来使用。在一个网络环境下，Windows 终端可以与传统 UNIX 终端、PC 灵活搭配，组成一个实用、经济、高效、安全的金融系统应用网络。

（2）所有的软件都在终端服务器上运行，终端仅仅是作为显示输出和数据输入的设备，终端上任何时刻断电都不会影响服务器上程序的运行和数据安全，在配置 UPS 时仅

给服务器配上 UPS 便可以了。

（3）正版的软件只要在服务器端安装一次，在整个系统中即可以使用，大大降低了软件的初始购置成本。

（4）完全集中式的网络管理，简化了工作环节，与传统的 PC 组网方式相比大大地减少了维护人员的工作量，一旦有事，网络管理人员不必到远端的服务器端检修，只需用一台终端以管理员身份登录到服务器上即可完成工作。

（5）大大降低了总体拥有成本。由于 Windows 终端完全基于服务器运行的特性，使得网络硬件升级换代的代价远远低于 PC 或无盘站，只需服务器端适当升级即可，终端本身不必考虑。

（6）Windows 终端支持终端开机自动连接功能。用户只要一开机，终端便会自动连到服务器上，还可以自动打开业务程序，简化了工作人员的工作，而且终端只需一次配置即可，以后几乎不需再次进行配置，应用人员只需简单地培训即可熟练掌握和正常使用。

（7）系统安全性得到大幅提高。Windows 终端本身不含硬盘、软驱和光驱，所有数据都保存在远端服务器端，有效地防止了重要数据的丢失和泄露，而且也不会像 PC 那样容易从外界染上病毒。同时可以提供多种安全控制机制，如根据用户的具体需求，加上 IC 卡安全模块等。

（8）具有较高的安全性。由于应用程序和数据都在服务器端运行和处理，如果终端突然掉电，数据并不会丢失，依然保持在服务器上，终端只要再次连到服务器上，还可以从断点处继续工作，不会影响正常的操作。

（9）整个系统安装调试简单、快速。

4.12.2　虚拟加密磁盘

磁盘加密技术是一种通过专门工具对磁盘的扇区磁道等进行加密的方法，而对加密磁盘的读写必须通过这个技术实现。PointSec 就是这样一种磁盘加密工具。它嵌入到操作系统中，对于使用者来说是完全透明的。而在使用 PointSec 加密的磁盘时，如果是挂到其他的计算机上，不用 PointSec 就无法调取数据。另外，使用者在正常使用时，必须知道密码，否则无法进入被 PointSec 加密的磁盘中进行操作。这种方式对于防止硬盘丢失情况下的数据保密是很有效的，对于企图不经允许而打开计算机进行操作和信息查阅也是很有效的。在已经打开计算机并进入了加密磁盘的情况下，任何接触到计算机的人或者在计算机上运行的软件，都可以对磁盘进行操作，本地桌面搜索工具也不例外，它可以直接对所有文件进行检索，并建立索引。如果这个索引不是建立在加密磁盘上，那么，本地加密磁盘上的数据就有可能泄露。虚拟磁盘技术经常是将一个文件映射为一个系统磁盘，通过操作系统对虚拟磁盘进行操作和对一个正常的磁盘驱动器或逻辑进行分区完全相同。虚拟磁盘技术和 PointSec 技术一样，在已经打开虚拟磁盘的情况下，任何程序或操作计算机的人都可以浏览查阅虚拟磁盘中的数据。本地桌面搜索工具可以直接

对所有文件进行检索，并建立索引。如果这个索引不是建立在加密磁盘上，那么，本地加密磁盘上的数据同样会泄露。

基于PGPdiks的虚拟加密盘的方法是在操作系统上以VxD方式增加设备管理的内核服务，从而为用户提供用于保存电子文档的虚拟盘，由于进行虚拟盘的电子文档均采用专门的技术进行加密，因此能够较好地解决其安全性要求。虚拟磁盘系统的基本操作如下：首先在物理硬盘上建立卷标文件；再以卷标文件为基础，设置虚拟硬盘的装载参数；待虚拟硬盘装载后，虚拟硬盘上的所有电子文档的存取操作都将交给虚拟硬盘驱动程序完成。通过在虚拟硬盘驱动程序中设置专门的加解密程序，来保证所存取的电子文档和数据的加解密操作。用程序通过使用动态加载的VxD，可以间接获得对Win9X/2000系统的控制权，Win9X/2000使用32位可安装文件系统（FIS），由可安装文件系统管理器（IFS Manager）来协调对文件系统和设备的访问，它接收以Win32API函数调用形式向系统发出文件I/O请求，再将请求转给文件系统驱动程序FSD，由它调用低级别的IOS系统实现最终访问。在完成文件I/O API函数参数的装配之后转相应的FSD执行之前，它会调用一个Hooker函数。通过安装自己的Hooker函数，就可以截获系统内对特定文件I/O的API调用，并进行相应的加解密处理，从而实现文件的安全存储。但从用户角度来说，完全屏蔽了底层的处理过程，当加载上该虚拟磁盘时，与使用普通的磁盘一样，用户可以很方便地进行各种操作。而装载虚拟硬盘时，首先将容器文件的前2048字节数据内容读入缓冲区，读入用户的密码组，可包括160个字符。采用SHA-1等算法获得密码组的摘要内容，以密码组的摘要值作为加密密钥。设置加密算法的初始向量，得到加密密钥和初始向量后，应用加密算法将缓冲区中读入的2048字节数据进行解密。在缓冲区的确定位置获得主密钥，其长度可变，可达256位。用主密钥的实际字长重新设置加密算法的初始向量，用主密钥将两组相同的随机数进行加密，并写入两个不同的区。重新装载时，需要将这两个区中的内容读出。利用前几步得到的密钥和初始向量，并通过相应的加密算法进行解密。如果对两个区解密的结果是相同的，则系统确认主密钥和初始向量组是合法的，此时可以用它初始化虚拟盘；否则，直接返回错误。初始化之后，对虚拟盘的操作将交给扩展的设备管理 VxD 处理。虚拟磁盘系统主要包括用户界面模块、密码处理模块和虚拟驱动程序模块三部分。其结构及用户界面模块如图4-131和图4-132所示。

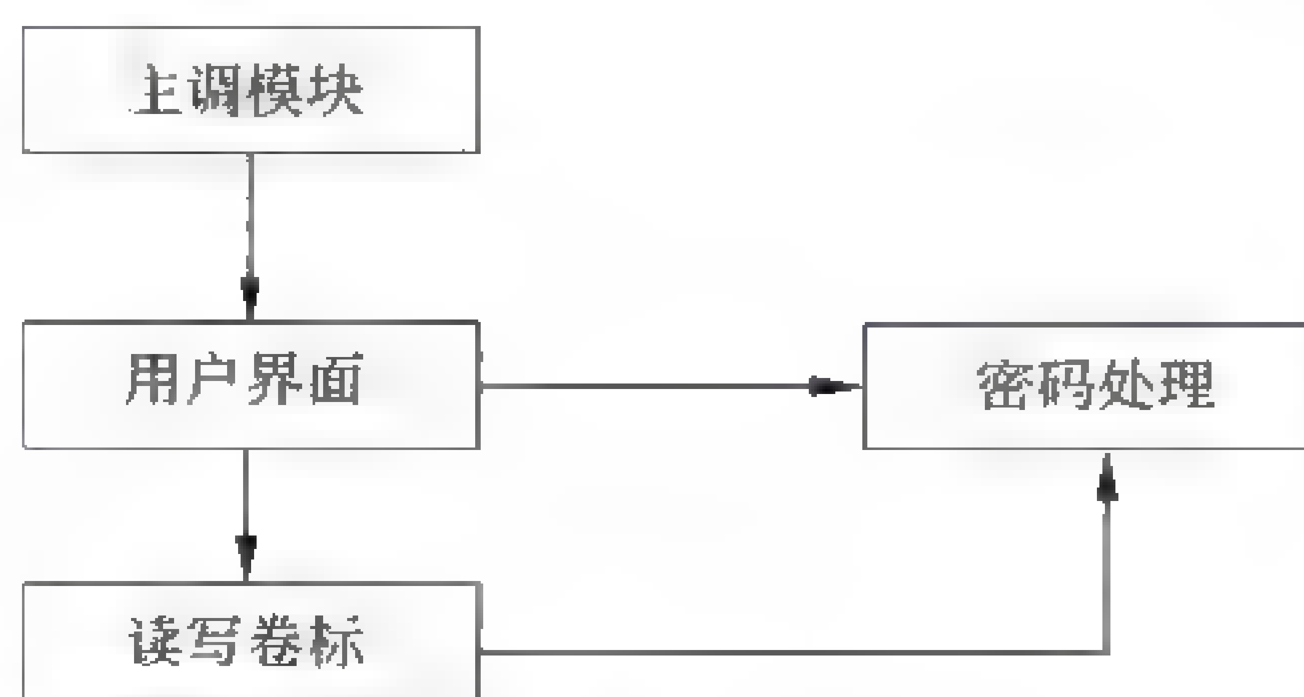


图4-131　虚拟磁盘系统结构

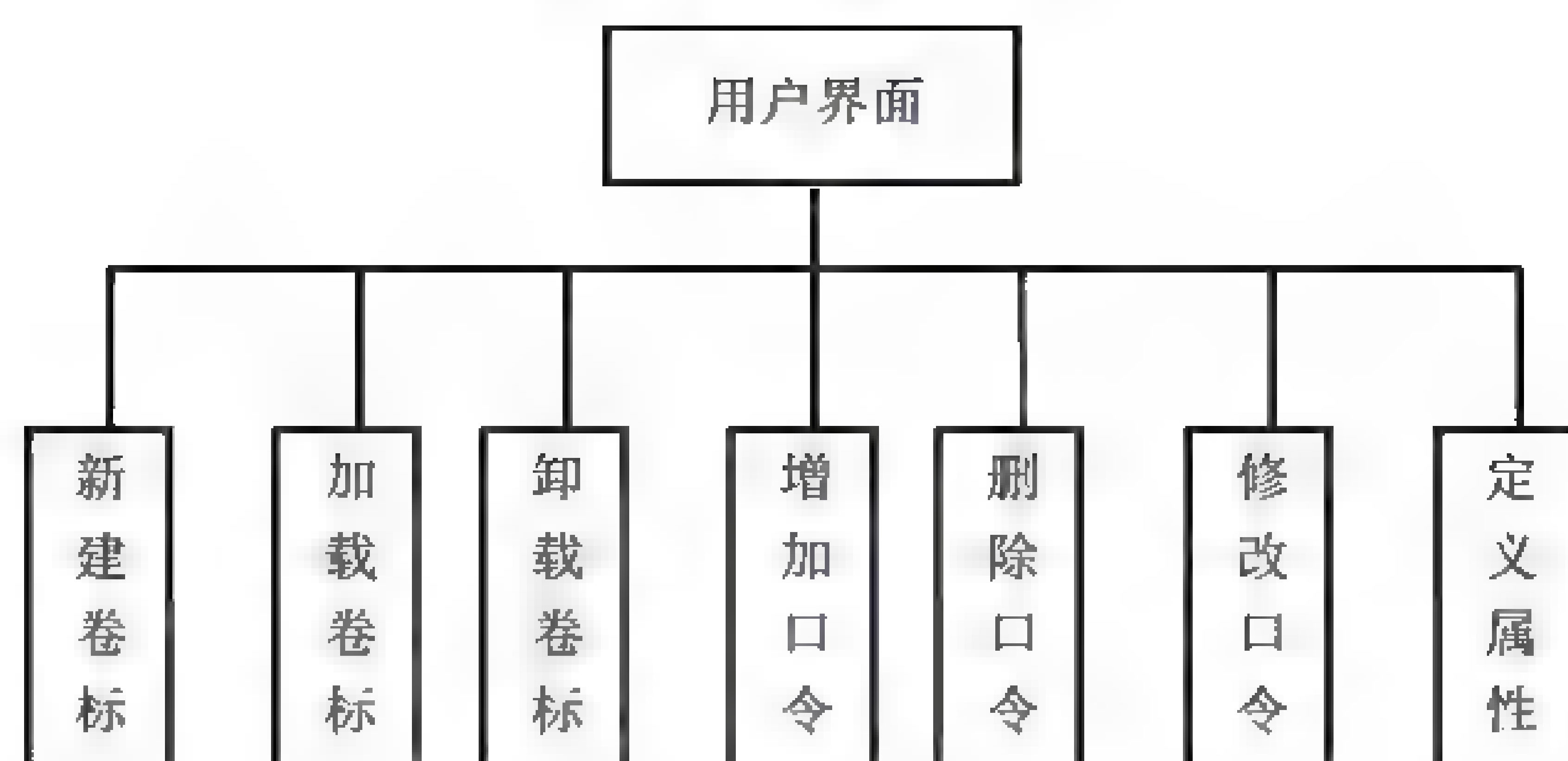


图 4-132　用户界面模块

用户界面主要是对该虚拟磁盘进行管理，包括以下功能。

（1）新建卷标。新建是指创建一个新的安全卷标和一个相关文件，以加密格式存储数据。用户可以定义新卷标的名字和存储路径，但需要选择所建虚拟盘的大小、单位、驱动符、密钥加密算法和数据加密算法等信息。同时，系统要求用户移动鼠标或敲击键盘取得随机数，将其作为随机数种子，然后用随机数生成算法生成一个会话密钥。用系统口令作为密钥，对会话密钥进行加密，将会话密钥密文存放在卷标文件的头部。

（2）加载卷标。当用户工作时，首先进行加载，选择想要加载的卷标，按要求输入对应的用户口令，并读出证书内容，就可以加载到某个虚拟驱动器上，然后可以在该驱动器中进行操作。

（3）卸载卷标。打开一个 PGPdiks 卷标称之为加载此卷标。同样，关闭卷标称之为卸载。每次用户使用完之后，应该卸载，否则可能会被别人查看到计算机上的数据。一旦卸载了卷标，其内容就被锁在了加密文件中。卷标的内容存储在加密文件中，直到再一次加载，否则其内容是不可访问的。

（4）增加口令。若允许其他人访问自己的加密磁盘，则只赋给读的权利，不允许其修改，可以为他设置一个不同的口令，以只读方式访问该虚拟磁盘。

（5）修改口令。首先输入要修改的口令，然后输入新口令，原口令就失效了。

（6）删除口令。输入要删除的口令，删除后该口令就失效了。

（7）定义属性。定义卸载卷标的各种方式。

密码处理模块主要是实现密码学的一些功能，包括的功能如下。

（1）产生随机数。PGP 使用了复杂的和强大的模式为不同的目的生成真随机数和伪随机数。

（2）生成密钥。用前面产生的伪随机数来生成会话密钥，用来加密虚拟磁盘内容。

（3）加解密处理。使用合适的加密算法，在对虚拟磁盘做读写操作时，需要对数据进行加解密，调用相应的函数来真正实现加解密操作。

在 Win9X 中对硬盘上的文件系统的访问采用分层模型，上层的驱动程序调用低层的

驱动程序，不同层的驱动程序完成不同的功能。最底层为硬盘驱动程序，它直接控制硬件。上层的驱动程序调用硬盘驱动程序访问硬盘，可以把硬盘看作一种连续存储介质，而不必关心硬盘的物理特性。硬盘上可能存在不同的文件系统，如 FAT 格式或 NTFS 格式。文件系统驱动程序向上提供访问文件系统的接口，对上层调用者来说，不必理会所访问的硬盘是什么格式。

4.12.3 终端硬件端口控制

USB（Universal Serial Bus，通用串行总线）用于将鼠标、键盘、移动硬盘、数码相机、VIP 电话或打印机等外设连接到 PC。理论上说，单个 USB host 控制器可以连接最多 127 个设备。USB 目前有两个版本：USB 1.1，最高数据传输率为 12Mb/s；USB 2.0，最高数据传输率提高到 480Mb/s。二者的物理接口完全一致，数据传输率上的差别完全由 PC 的 USB host 控制器以及 USB 设备决定。USB 可以通过连接线为设备提供最高 5V，500mA 的电力。USB 接口有三种类型：一般用于 PC 的 Type A、用于 USB 设备的 Type B 和用于数码相机、数码摄像机、测量仪器以及移动硬盘等设备的 Mini-USB。通过 USB 接口泄密已经是计算机内部网络信息泄露发生的一个重要途径，随着科技的迅速发展，大量的 USB 端口设备出现，如 U 盘、移动硬盘、移动刻录机以及其他 USB 接口的存储设备，这在方便了信息传递的同时，也为将信息从计算机本机或者网络内部的信息非法复制出去创造了一个方便的条件。涉密 USB 移动存储介质和非密 USB 移动存储介质交叉使用，应用于不同密级、不同安全域的 USB 移动存储介质交叉使用，都会带来泄密的可能。很多病毒利用 USB 移动存储介质做为传播媒介，通过病毒的传播而造成泄密。移动存储介质发生故障时，存有涉密信息的介质不经处理或无人监督就带出修理，或修理时没有人员在场监督，而造成泄密。为防止非法用户从企业内部和个人 PC 上盗取重要文件或资料，对软驱、光驱、USB 接口上的存储设备进行监控的任务迫在眉睫。USB 的优点在于 USB 控制器只占用一个 IRQ，而其他联机的 USB 设备则都不需 IRQ。不需要使用跳线去调整或修改硬件设置，来指定要使用哪一个 USB 设备。在设置硬件上也非常的容易，即插即用（plug-and-play）操作系统会自动安装必要的驱动程序。USB 设备都使用相同的接头，减少了消费者的麻烦。USB 能在同一端口上支持多台设备。技术上一个 USB 端口能够支持最大 127 台设备同时联机，不过要用 USB Hub 这类辅助装置把这些设备都接上。USB 的带宽是由整个通道上的设备共享的，所以要是部分外设保留了部分的带宽，能安装的外设数也自然跟着减少。为了获得更高的 USB 带宽，需要增加额外的 USB 端口数，通常通过加装 PCI 接口卡来增加可用的 USB 端口数。USB 界面设备主要有键盘、鼠标、游戏控制器、摄像机、存储装置、扫描仪和其他外设。计算机上所需要的外设，大多都有 USB 的版本。

IEEE 1394 具有廉价、占用空间小、速度快、开放式标准、支持热插拔、可扩展的数据传输速率、拓扑结构灵活多样、完全数字兼容、可建立对等网络、同时支持同步和

异步两种数据传输模式等特点。IEEE 1394 网络具有以下主要特点和局限。

（1）节点之间的最大距离不能超过 4.5m，可以使用 IEEE 1394 中继器克服这一局限，一台 IEEE 1394 中继器可以将节点之间的距离延长 4.5m。因为 IEEE 1394 最多只能支持 16 层树形网段，所以两个端点之间的最大距离为 72m。

（2）每个网段最多可以连接 63 台设备，每台 IEEE 1394 可以连接 10231394 个网段，从而可以实现各种复杂的网络结构。不过考虑到两个节点之间 4.5m 的最大距离限制，IEEE 1394 并不适合在广域网中使用。

（3）因为 IEEE 1394 设备支持热插拔，所以可以在任何时候向 IEEE 1394 网络添加或拆除设备，既不用担心影响数据的传输，也不需要进行重新配置系统，可以根据变化的环境进行自动调节。

（4）IEEE 1394 网络使用的是对等结构，不需要设置专门的服务器，不过对于那些集中进行管理或数据存储的系统来说，IEEE 1394 并不是一个理想的选择。

（5）同一网络中的数据可以不同的速度进行传输，目前可以实现的速度为 100，200 和 400Mbps。这一特点决定了在设计网络时，一定要考虑到不同设备的传输性能。如果在两台传输速度可达 400Mbps 的设备之间放置一台 100Mbps 的设备，无疑会使实际的传输速度大打折扣。

IEEE 1394 在技术上做了进一步的改进，在保持与已有产品兼容的同时，使 IEEE 1394 的互操作性和控制性能得到了较大的提高。与前一次修改不同，IEEE 1394 代表的是一次巨大的变革，它承诺将把数据传输速度提高到 800Mbps 和 1.6Gbps，而且新版本的设计人员称这种体系结构的底层数据速率能达到 3.2Gbps 甚至更快。同时新版标准还克服了旧版本允许的最大电缆长度的局限性，新的传输介质和增强的仲裁技术将使每个中继段的最大距离得以大大加长，从原来的小于 5m 延长到超过 100m。此外，新版本还承诺提高系统的管理能力，如在系统重新启动后能够以更快的速度对总线进行重新配置。一个完整的 IEEE 1394 接口分为两个硬件层和三个协议层，其中物理层和连接硬件层的实现可以是一组芯片或者一块单独的芯片。最底层的协议层，即传输层，通常由一个固件来实现，其他各协议层则完全以软件的形式实现。由于引进了一种称为 Betamode 的新的物理层配置，IEEE 1394 实现了较高的操作速度。Betamode 是在 IBM 的 8810B 编码之上进行了改进，8810B 编码过去用在其他一些高性能的串行总线技术中。新的编码机制中增添了一些控制代码，在确定传输内容的完整性之后，这些控制代码可以很容易从数据中分离出来。

作为一种数据传输的开放式技术标准，IEEE 1394 被应用在众多的领域。目前 IEEE 1394 技术使用最广的是数字成像领域，支持的产品包括数字相机或摄像机等。无论是在计算机硬盘还是网络互连等方面都有其广阔的用武之地，最近 Evergreen 公司推出的 HotDrive 硬盘就采用了 IEEE 1394 技术。尽管 IEEE 1394 目前还没有被 PC 厂商所广泛采用，但是其在数字成像领域内的重要作用已经被世人所关注。作为业界领头羊的

SONY，身先士卒地在数字相机、数字摄像机、笔记本计算机甚至桌面 PC 等众多的产品中对 IEEE 1394 技术提供了全面的支持。作为 IEEE 1394 标准开发者的 Apple 公司对其也是倾注了极大的心血，此外软件业巨头 Microsoft 也已经开始了面向 IEEE 1394 的产品开发，无疑这将会大大推动 IEEE 1394 技术的普及和推广。

因为 IEEE 1394 和 USB 使用的都是串行接口，而且都支持热插拔，所以人们很容易将两者进行对比。其实两种技术之间还是存在着非常显著的区别。不能将其视为简单的竞争关系，它们都有各自的适用领域。USB 1.1 支持的最大数据传输速度为 12Mbps，USB 2.0 支持的最大数据传输速度为 480Mbps。USB 需要主机 CPU 对数据传输进行控制。与 USB 不同，IEEE 1394 允许每台设备的最大传输速度可以达到 400Mbps、800Mbps、1.6Gbps 甚至 3.2Gbps，不需要任何主机进行控制，可以同时支持同步和异步传输模式。因此，可以看出 USB 的市场定位是那些对数据带宽要求相对较低的产品，如鼠标和打印机等，而 IEEE 1394 则更适合于那些数据传输量更大的设备，如视频设备或计算机硬盘等。

IEEE 1394 开放式主控制器接口 OHCI 是向所有准备支持 IEEE 1394 技术的厂商提供的开放式标准。OHCI 由物理层、链路层、交易层和串行总线管理 4 个部分组成。物理层提供设备和线缆之间的电气和机械连接、处理数据传输和接收、确保所有设备可以正常访问总线，物理层功能由硬件实现。链路层提供同步和异步模式下的数据包接收、确认、定址、数据校验以及数据分帧等，链路层功能由硬件实现。交易层只处理异步数据包，提供 Read、Write 和 Lock 命令，Read 命令向命令发出方传回数据，Write 命令向接收方发送数据，Lock 命令通过生成往返通路实现 Read 和 Write 功能，交易层功能由固件实现。串行总线管理提供全部总线的控制功能，包括确保向所有总线连接设备的电力供应，优化定时机制，分配同步通道 ID，以及处理基本错误提示等。在实际操作过程中，设备必须首先要求控制物理层。如果进行异步传输数据，发送和接收方互换地址，然后进行数据传输。当接收方收到数据包时，会向发送方传回确认信息。如果接收方没有收到数据包，则启动错误修复机制。如果进行同步传输，发送方首先要求获得一个特定带宽的数据通道，然后将通道 ID 附加在所要传输的数据中一起发送，接收方对数据流进行检测，只有当发现具有特定 ID 号的数据时才进行接收。同步数据传输模式在优先级上要高于异步传输模式，当一台设备发送同步数据时，将获得一个专用的数据通道，直到数据传送完毕为止。而同一时刻发生的异步数据传输则只能使用当前所剩的可用带宽。上述机制充分保证了像视频流这样的对时间延迟要求很高的应用，可以在不受其他应用干扰的情况下实时完成。在 OHCI 规范中，没有任何对数据调制或解调的规定，这是因为 IEEE 1394 是一种全数字协议，在数据传输过程中不需要进行任何的数模转换，从而大大节省了系统开销。

随着 PC 行业与通信和其他媒体之间的合作逐步深入，人们越来越需要一个统一的接口标准。IEEE 1394 可以满足所有各方的需要，而且成本低，易于实现。IEEE 1394 已

经在多媒体领域被广为接受，相信在急需一种可以把内部设备如硬盘和外部设备如数字相机连为一体的新型高速总线的 PC 市场，IEEE 1394 的前景也必将是一片光明。目前的问题不是 IEEE 1394 是否能够被接受，而是众多的硬盘和主板厂商是否愿意做出转变的抉择，一些主板厂商已经开始在其产品中融入 IEEE 1394 技术，但是好像硬盘厂商的步伐有些滞后，不过完全有理由相信 IEEE 1394 有一天终将会成为新的总线标准。

PCMCIA（Personal Computer Memory Card International Association）又称 PC card，有 Type Ⅰ、Type Ⅱ和 Type Ⅲ三种标准，分别规定了所用 PC 卡的尺寸及相应的电路等。当前有三种 PC 卡标准，它们的长宽都是 85.6mm×54mm，但厚度不一样：Type Ⅰ是最早的 3.3mm 厚卡；Type Ⅱ将厚度增至 5.0mm；Type Ⅲ则进一步增大厚度到 10.5mm。一段时间以来，Type Ⅰ几乎只在内存设备中应用。但最近 Modem 和其他设备也开始相继采用 Type Ⅰ标准。Type Ⅱ是当今最占优势的一种尺寸，用于大多数设备。更厚的 Type Ⅲ卡则主要用于微型硬盘驱动器，这种驱动器已变得越来越普遍。由于这三种卡共用同样的总线连接器，所以较薄的卡可顺利安装到为较厚的卡设计的插槽。制订自己的标准时，PCMCIA 采纳了“日本电子工业开发协会（JEIDA）”的一些设计思想，规定了内存卡的物理设计方案、计算机插槽设计方案、电气接口以及相关软件，该标准最新的版本已集成了 PCMCIA 和 JEIDA，使产品间的兼容性有了进一步的提高。PC 卡现已应用于多种场合，其中包括几种类型的 RAM 内存、预编程 ROM 卡、Modem、声卡、软盘控制器、硬盘驱动器、CD-ROM 和 SCSI 控制器、全球定位系统（GPS）卡、数据采集卡、LAN 卡、传呼机等。还处在发展初期，PCMCIA 市场就显示出蓬勃发展的气象。PCMCIA 标准使 PC 卡能在多种类型的计算机中使用，无论它采用的是何种微处理器。PC 卡不仅可以插到计算机上，也可用于其他数字化设备，如测试仪器、数码成像设备及工业控制器等等。系统制造商、周边设备制造商、零售商和系统用户均可从中获益。随着便携式计算机系统（含笔记本、亚笔记本、掌上型以及 PDA）的广泛应用，对便携式扩展设备的要求也越来越迫切。在扩展卡标准制定之前，计算机能采用的周边设备（如插卡式内存和 Modem 等）通常都是专用的，不可换成其他厂家的类似产品。许多像 Modem 这样的设备更是只能插入一台特定型号的计算机，即便同厂出品的其他型号也不能使用。通常，这些周边设备并不设计成可与其他计算机互换，而是作为一种固定设计提供，只适合最初装配的那种计算机。

PCMCIA 标准的问世已有些时日，目前已出至第三版。其间进行了大量必要的变动与改进，以适应系统和 PC 卡制造商不断变化的需求。 PCMCIA 标准的发展已完全超出了最初定义内存卡的范围，现在包括的外设类型有存储器类（硬盘驱动器、内存卡）、接口类（CDROM/DVD 接口、并串口、扩展接口卡）、网络通信类（以太/令牌网卡、无线/红外局域网卡、Modem 卡、ISDN 卡、移动电话卡）和多媒体类（声卡、视卡、游戏摇杆卡、电视/广播接收卡及视讯会议卡等）。最早的版本是 1.0，建立的标准主要面向类似现在的 RAM 卡那样的内存卡。2.0 到 2.1 版则增加了“卡和插槽服务（Card and Socket

Services）”软件规范、ATA（AT 附件，涉及 PC 卡上的 IDE 驱动器接口）规范和 AIMS（自动索引海量存储，是一种在 PC 卡上保存图像和多媒体数据的标准，通常用于照 / 摄像技术）规范。最新的 PCMCIA 版本实际叫做 PC Card Specification（PC 卡规格），有时也不十分恰当地称为“3.0 版”。这一版本提供了对 DMA（直接内存存取）、更高速多媒体应用、即插即用、多功能卡以及 CardBus 的支持。这一版本也允许用 3.3V 的逻辑电压设计 PC 卡和系统。由于能节省电池供电设备的能源，3.3V 逻辑电平日趋流行。PCMCIA 标准的每一次新发布，都力求做到与旧版本保持向后兼容。CardBus 对 PCMCIA 总线结构进行了重新定义和改进，但仍可回复到以前在第 1 和第 2 版制订的标准。CardBus 的主要目的是将 PCMCIA 总线扩展到更高的速度，以便连接功能更强的设备，并提供对 32 位 I/O 及内存数据通道的支持。它包括了一个新的屏蔽总线连接器，且不可将 CardBus 卡插入为 2.x 或更旧版本设计的上一代系统。

在大多数提供了 PC 卡插槽的新计算机中，同时采用了卡和插槽服务（Card and Socket Services）软件，在计算机与 PC 卡之间提供一个标准化的软件接口。简单地说，卡和插槽服务软件之于 PC 卡，便如同 DOS 和 BIOS 之于 PC。初级系统仅用插槽服务来实现与 PCMCIA 硬件的连接，需为每种类型的 PC 卡安装专用的驱动程序。而在某些新操作系统中（如 Win95），已集成了 Card 和 Socket Services 的功能。若无意外，这似乎应成为未来的一种趋势，可将安装时的麻烦减轻到最低程度。但是，无论如何都要为某些 PC 卡提供独立的设备驱动程序，因为没有一种操作系统能预测到未来 PC 的每一项功能与配置。大多数计算机系统也针对 PC 卡的热插拔进行了特殊设计（在不关闭计算机电源的情况下插拔 PC 卡），使用户在不打断自己工作或者不退出当前程序的前提下连接或断开设备。例如，可拔掉 Modem 卡，重新插入一张 RAM 卡，不必为此而关闭计算机。新卡装好以后，计算机的插槽硬件会发出相应的通知，以便系统接纳新的周边设备。相反，若将卡拔掉，硬件会侦测到这一情况，并通知软件不可再使用该卡和自动采取适当的行动。一旦插入或拔掉一张卡，许多计算机都会用自己的喇叭发出熟悉的哔哔声。尽管 PC 卡制造商遵守的规范已进行了兼容性方面的全面设计，但仍应注意到许多计算机系统并不一定采用的是最新软件版本（Card 和 Socket Services）。某些情况下，当新型 PC 卡与旧版本的“卡和插槽服务”软件共用时，会出现兼容性方面的问题。有些 PC 卡产品则配套提供了“卡和插槽服务”的最新版备份，一旦现有软件属于过期版本，且侦测到兼容问题，就会自动安装新版本的服务。新版本的“卡和插槽服务”软件通常也可以从计算机厂商以及其他公司获得，正如早先指出的那样，时下最新的潮流是将“卡和插槽服务”的功能直接集成到操作系统内部。

目前市场上的桌面安全系统主要有信安世纪 Desksafe 2.0、清华紫光 S 锁、华为聚合式桌面安全解决方案、Broadview DCC 桌面安全解决方案和趋势科技推广企业桌面安全解决方案等。

Desksafe 2.0 是一款面向政府、企业的桌面安全产品，能够实现针对文件与目录的安

全功能文件的加密和签名、文件的解密和验证、目录的加密和签名、目录的解密和验证和文件安全删除。DeskSafe 软件套件的 MailSafe 组件是电子邮件的安全组件，主要功能有发送加密邮件、发送签名邮件、收取阅读加密邮件、验证阅读签名邮件、并能通过文件安全模块加密、解密、签名、验签名附件等。DeskSafe 软件套件的 MailSafe 安装后在浏览器工具栏产生加密和签名动作按钮，用户只需选择这两个按钮即可发送安全的电子邮件，无须改变以前的使用习惯。另外，DeskSafe 能够自动到指定的服务器寻取接收者的数字证书，无须用户烦琐的手工搜索、导入等操作。DeskSafe 在支持微软操作系统的书库的同时，还能够支持 USB-KEY 密钥存储能够带给用户更高的安全性。该产品为基于 Internet/Intranet 的电子邮件用户建立起了一种易用的、崭新的、可信赖的系统，防止了电子邮件中重要信息的泄露和失密，给那些希望保护自己邮件信息安全的用户提供了完美的选择。

清华紫光 S 锁是一种保护计算机重要文件不被非法窃取、浏览、篡改、删除或破坏的信息安全产品。紫光 S 锁是一套基于 UBS 硬件标准的安全升级套件，它的外观与 U 盘相同，实际上是一台没有输入输出设备、只带有 UBS 接口的超小型计算机。其内部集成了包括中央处理器、加密运算协处理器、只读存储器、随机存储器、电可擦除可编程只读存储器等，以及固化在 ROM 内部的芯片操作系统 COS（ChipOperating System)、硬件 ID 号等。支持 ISO 7816 T=0 通信协议；内置硬件随机数发生器；支持 RSA1024 位、ECC160 位/192 位公钥密码算法，直接在芯片内生成 RSA 或 ECC 密钥；同时也支持 DES、3DES 密码算法、MD5、SHA-1 数据散列算法。采用了通过中国人民银行认证的 SmartCOS，其安全模块可防止非法数据的侵入和数据的篡改，防止非法软件对 S 锁进行操作。通过 UBS 安全子系统和安全 COS（芯片操作系统）给计算机配置一个封闭、安全的运行环境，从硬件级上解决了计算机身份认证和文件保密等安全问题。2004 年 1 月，无锡华网科技推出了 JX-KEY 桌面安全系统，其采用密码学技术和软件硬件结合的方法，对个人计算机进行信息的安全保护，是可将普通 PC 轻松升级为安全计算机的信息安全产品。JX-KEY 对保存到文件保险箱中的文件自动进行加密，对访问文件保险箱的用户进行口令和硬件双重身份认证。JX-KEY 电子钥匙采用智能卡+USB 读卡器集成的结构，能实现智能卡的功能。其主要技术指标如下。

（1）符合 CSP 和 PKCS#11 技术标准。

（2）其中的 COS 符合中国人民银行 BPOC 检测规范。

（3）支持数字证书、密钥存储以及加密解密算法的实现。算法包括对称算法（DES、3DES、RC2、RC4)、公私钥算法、摘要算法（MDS、SHA-1）和数字签名算法。

（4）支持真随机数发生器，支持密钥的产生。

随着网络技术的发展，远程、移动、协同办公和因特网接入被现代企业广泛采用。这些新工作方式的采用在带来更多资讯和更高生产效率的同时也给企业办公网络带来更多的信息安全问题，如病毒、终端滥用资源、非法接入、非授权访问、终端安全漏洞、

恶意终端破坏、信息泄密及安全策略无法有效落实等。传统的基于网关的安全架构都只是针对个别的问题，而没有构造出一个能彻底解决企业网络安全问题的平台。聚合式桌面安全解决方案采用先进的技术开发手段和工程管理方法，以核心自产软件为平台，统一整合和管理各终端安全软件，并与接入控制网关硬件联动进行网络层接入控制，实现内部办公网络及分支机构等对内控安全需求的全面内网安全解决方案。聚合式桌面安全解决方案运行稳定可靠，很好地保障企业内部网络的稳定和安全，保证了业务的顺畅运行。聚合式桌面安全解决方案充分考虑企业网络的现状和安全管理需求，为企业建立起主动自我防御、安全加固的自免疫安全系统，提高企业网络系统的整体安全水平，为企业的长期稳定发展保驾护航。系统支持基于账户的接入认证功能，用户账户决定其权限和策略，可以灵活方面地满足移动办公用户和外地出差用户的接入认证和网络访问。可采用用户名加口令、MAC 地址、AD 域认证多种认证方式，还提供设备指纹（硬盘序列号、MAC 等）与用户绑定的安全认证方式，保证了认证的可信度。系统的设计开发完全遵循国际和国内的相关行业标准和软件工程管理规范，采用通用化和模块化设计，服务器端采用专用端口和协议，提供标准接口与各种安全防护软件联动，构建了一个完整的网络安全体系架构。检查—隔离—加固—管理的整体解决思路，实现企业内部网络安全自免疫。安全接入控制网关可灵活部署在需要控制的企业网络范围内，支持分布式部署，支持直挂或旁挂；桌面安全管理服务器可灵活部署在企业网络的任何地方，客户端软件可通过网络自动升级，强大的软件分发功能为补丁和软件升级提供保证，提供完善的双机热备功能。审计人员和管理人员的职能划分采取了分级分权管理，确保每一个人的操作都会被审计、被监控，从而保证了使用的安全性。系统提供非常方便的各种日志的查询功能，多种形式的审计报表，帮助审计人员更好地完成审计工作。聚合式桌面安全解决方案给用户提供的功能：强制认证、安全防护、安全监控和资产管理。安全策略服务器和安全接入控制网关联动，控制终端的网络访问权限，对不同的用户，不同安全状况的用户开放不同的权限。通过对终端实施身份认证和安全性认证的双重认证检查，保证访问企业网络资源的终端为拥有合法身份同时自身安全状况是符合企业安全策略的终端，隔离不安全终端并提供相应的安全修复，帮助企业进行终端安全加固，为企业内网提供全面的终端安全防护，防止病毒传播、终端滥用资源、非法接入、非授权访问和终端安全漏洞。根据企业安全策略对内网中的终端行为实施监控，跟踪终端进程，控制QQ、MSN 和游戏软件的使用，监控上网记录，监控 USB 存储设备，监控拨号外联等，帮助企业提高工作效率，杜绝终端恶意破坏，保卫企业内网安全、防止企业信息泄密。提供对企业终端硬件和软件资产信息的跟踪管理和查询，帮助企业实现终端资产可控可管。

Broadview DCC 桌面安全解决方案是为企业管理者量身定做的联网桌面终端综合管理平台，其在设计时就遵循了 ITIL/ITSM 规范及公安部信息安全标准等原则，切实总结了近 5 年来国内企业 IT 管理的实际需要，参照国内客户的网络结构、终端特点和管理模

式，了解国内用户各种已有的管理产品，并结合技术发展的趋势，以此定位产品的架构、性能、功能和管理界面，使 Broadview DCC 成为一款具有符合国内企业 IT 架构和管理模式，且真正适合用户最迫切需求的桌面系统管理平台。

趋势科技推广企业桌面安全解决方案率先获 Windows Vista 认证。当前许多病毒开始伪装入侵 Web，即使在网关端设置阻止执行文件进入，恶意程序也可能伪装成 txt、jpg 和 gif 文件入侵，这些在网关端都无法阻挡。病毒的入侵，刺激着杀毒厂商不断升级旗下产品。网络安全软件厂商趋势科技日前宣布，将 Web 信誉服务加入网络版安全套件 OfficeScan 8.0、互联网网关安全设备 IWSA3.1 以及 Interscan 网关安全设备 IGSA1.5 中，分别针对客户端、服务器和网关进行防护，防止使用者存取含有恶意程序的相关网站。作为第一套融合新型网络信誉技术的企业解决方案，OfficeScan 8.0 是首款获得微软 Windows Vista 认证的企业桌面安全解决方案。该解决方案将通过增加网络安全等级与得到增强的反间谍技术加强对网络威胁的防护。移动用户经常从诸如飞机场、旅馆等远程设施环境连接到因特网，所以 OfficeScan 8.0 将采用 Web 信誉服务技术保护扩展至企业网络之外，通过基于个人 DNS 域名信誉进行动态评估的新型技术来保护网络的多种终端设备。通过分析网络域名获得的被访问网页的可信度，WRS 将为网页评定“信誉等级”。WRS 由全球超过 150 台在线服务器 7×24 小时进行在线实时分析，评定的准确率高达 98%。WRS 会提供实时更新，如果遭到恶意程序入侵的网站已修复，评定分数也会立即恢复，不会影响到使用者点击进入正常网页。加入了 WRS 信誉服务后，OfficeScan 8.0 除了监测入口网站外，也可以检查内网，以 URL 的形式侦测，能够更精准地防止使用者不小心下载到恶意程序。现在用户如果利用 Google 搜索到被植入恶意程序的网页时，也会出现警告，但只针对入口网站，而且若不用 Google 搜寻而是直接输入网址，还是会中毒，但 OfficeScan 8.0 不会出现这样的情况。此外，OfficeScan 8.0 提供给用户 4 种安全等级，企业可依需求自行设定。判断标准则依网络域名历史、网络域名稳定度、网络域名关联性等加以判断。OfficeScan 8.0 具备实时扫描功能，当使用者新增、移除或接收档案时，系统就会启动实时扫描。

4.13 系统安全

4.13.1 DMZ

DMZ 是为了解决安装防火墙后外部网络不能访问内部网络服务器的问题而设立的一个非安全系统与安全系统之间的缓冲区。这个缓冲区位于企业内部网络和外部网络之间的小网络区域内，在这个小网络区域内可以放置一些必须公开的服务器设施，如企业 Web 服务器、FTP 服务器和论坛等。整个需要保护的内部网络接在信任区端口后，不允许任何访问，实现内外网分离，达到用户需求。来自外网的访问者可以访问 DMZ 中的

服务，但不可能接触到存放在内网中的公司机密或私人信息等，即使 DMZ 中服务器受到破坏，也不会对内网中的机密信息造成影响。DMZ 更加有效地保护了内部网络，因为这种网络部署，比起一般的防火墙方案，对攻击者来说又多了一道关卡。网络设备开发商利用这一技术开发出了相应的防火墙解决方案。DMZ 通常是一个过滤的子网，DMZ 在内部网络和外部网络之间构造了一个安全地带。DMZ 防火墙方案为要保护的内部网络增加了一道安全防线，它提供了一个区域放置公共服务器，从而又能有效地避免一些互联应用需要公开但与内部安全策略相矛盾的情况发生。在 DMZ 区域中通常包括堡垒主机、Modem 池以及所有的公共服务器，但要注意的是电子商务服务器只能用作用户连接，真正的电子商务后台数据需要放在内部网络中。在 DMZ 防火墙方案中，一般包括两个防火墙，外部防火墙抵挡外部网络的攻击，并管理所有内部网络对 DMZ 的访问。内部防火墙管理 DMZ 对于内部网络的访问。内部防火墙是内部网络的第三道安全防线（前面有了外部防火墙和堡垒主机），当外部防火墙失效时，它还可以起到保护内部网络的功能。而局域网内部，对于 Internet 的访问由内部防火墙和位于 DMZ 的堡垒主机控制。在这样的结构里，一个黑客必须通过三个独立的区域（外部防火墙、内部防火墙和堡垒主机）才能够到达局域网。攻击难度大大加强，相应内部网络的安全性也就大大加强，但投资成本也是最高的。在实际的运用中，某些主机需要对外提供服务，为了更好地提供服务，同时又要有效地保护内部网络的安全，将这些需要对外开放的主机与内部的众多网络设备分隔开来，根据不同的需要，有针对性地采取相应的隔离措施，这样便能在对外提供友好服务的同时最大限度地保护内部网络。针对不同资源提供不同安全级别的保护，可以构建一个 DMZ 区域，DMZ 可以为主机环境提供网络级的保护，能减少为不信任客户提供服务而引发的危险，是放置公共信息的最佳位置。在一个非 DMZ 系统中，内部网络和主机的安全通常并不如人们想象的那样坚固，提供给 Internet 的服务产生了许多漏洞，使其他主机极易受到攻击。但是，通过配置 DMZ 可以将需要保护的 Web 应用程序服务器和数据库系统放在内网中，把没有包含敏感数据、担当代理数据访问职责的主机放置于 DMZ 中，这样就为应用系统安全提供了保障。DMZ 使包含重要数据的内部系统免于直接暴露给外部网络而受到攻击，攻击者即使初步入侵成功，还要面临 DMZ 设置的新的障碍。

当规划一个拥有 DMZ 的网络时，可以明确各个网络之间的访问关系，确定如下访问控制策略。内网可以访问外网，内网的用户显然需要自由地访问外网。在这一策略中，防火墙需要进行源地址转换。内网可以访问 DMZ，此策略是为了方便内网用户使用和管理 DMZ 中的服务器。外网不能访问内网，内网中存放的是公司内部数据，这些数据不允许外网的用户进行访问。外网可以访问 DMZ，DMZ 中的服务器本身就是要给外界提供服务的，所以外网必须可以访问 DMZ，同时，外网访问 DMZ 需要由防火墙完成对外地址到服务器实际地址的转换。DMZ 不能访问内网，如果违背此策略，则当入侵者攻陷 DMZ 时，就可以进一步进攻到内网的重要数据。DMZ 不能访问外网，此策略在一些特

殊情况下（例如 DMZ 中放置邮件服务器时，就需要访问外网，否则将不能正常工作）除外。在网络中，非军事区是指为不信任系统提供服务的孤立网段，其目的是把敏感的内部网络和其他提供访问服务的网络分开，阻止内网和外网直接通信，以保证内网安全。

DMZ 提供的服务是经过了地址转换和受安全规则限制的，以达到隐蔽真实地址、控制访问的功能。首先要根据将要提供的服务和安全策略建立一个清晰的网络拓扑，确定 DMZ 区应用服务器的 IP 和端口号以及数据流向。通常网络通信流向为禁止外网区与内网区直接通信，DMZ 区既可与外网区进行通信，也可以与内网区进行通信，受安全规则限制。DMZ 区服务器与内网区、外网区的通信是经过网络地址转换实现的。网络地址转换用于将一个地址域（如专用 Intranet）映射到另一个地址域（如 Internet），以达到隐藏专用网络的目的。DMZ 区服务器对内服务时映射成内网地址，对外服务时映射成外网地址。采用静态映射配置网络地址转换时，服务用 IP 和真实 IP 要一一映射，源地址转换和目的地址转换都必须要有。安全规则集是安全策略的技术实现，一个可靠、高效的安全规则集是实现一个成功、安全的防火墙非常关键的一步。如果防火墙规则集配置错误，再好的防火墙也只是摆设。在建立规则集时必须注意规则次序，因为防火墙大多以顺序方式检查信息包，同样的规则，以不同的次序放置，可能会完全改变防火墙的运转情况。如果信息包经过每一条规则而没有发现匹配，这个信息包便会被拒绝。一般来说，通常的顺序是，较特殊的规则在前，较普通的规则在后，防止在找到一个特殊规则之前一个普通规则便被匹配，避免防火墙被配置错误。DMZ 安全规则指定了非军事区内的某一主机（IP 地址）对应的安全策略。由于 DMZ 区内放置的服务器主机将提供公共服务，其地址是公开的，可以被外部网的用户访问，所以正确设置 DMZ 区安全规则对保证网络安全是十分重要的。FireGate 可以根据数据包的地址、协议和端口进行访问控制。它将每个连接作为一个数据流，通过规则表与连接表共同配合，对网络连接和会话的当前状态进行分析和监控。其用于过滤和监控的 IP 包信息主要有源 IP 地址、目的 IP 地址、协议类型（IP、ICMP、TCP、UDP）、源 TCP/UDP 端口、目的 TCP/UDP 端口、ICMP 报文类型域和代码域、碎片包和其他标志位（如 SYN、ACK 位）等。为了让 DMZ 区的应用服务器能与内网中 DB 服务器（服务端口 4004、使用 TCP 协议）通信，需增加 DMZ 区安全规则， 这样一个基于 DMZ 的安全应用服务便配置好了。其他的应用服务可根据安全策略逐个配置。DMZ 无疑是网络安全防御体系中重要组成部分，再加上入侵检测和基于主机的其他安全措施，将极大地提高公共服务及整个系统的安全性。

内部网络和主机的安全通常并不是那样的坚固。在一个非 DMZ 系统中，提供给 Internet 的服务产生了许多漏洞，使其他主机极易受到攻击。解决问题的方法之一是把没有包含敏感数据，担当代理数据访问职责的主机放置于 DMZ 中。通过应用程序的接口（如 Web 站点），或通过网络协议（如 HTTP）可以实现上述方法。在网络中数据从应用

层分离提供了附加的安全，因为实施 DMZ 的系统不会把包含商业数据的内部系统直接暴露给网络攻击。攻击者取得初步入侵成功后，要面临 DMZ 设置的新障碍。一个 DMZ 配置提供了实施附加安全措施的自然层，诸如主机加固和网络或基于主机的入侵检测。主机加固是配置主机系统的过程，因此它比默认的配置要安全的多。主机安全的实施提高了攻击者入侵的难度。作为一个 IT 管理者，你可以要求企业中的所有系统符合严格的加固的安全需求。然而，你也可以坚持基于 DMZ 系统这样的需求，因为它们是现存系统的一个小子集，因而在管理和维护这样高安全配置的系统，不需要付出太多努力。一个带有入侵检测的 DMZ 配置可以添加重要的安全利益。最显著的一点是，DMZ 为管理人员节省了响应攻击的时间，因为通过网络访问控制攻击被隔离在内部系统外面，数据资源和设备在其他的地方，因此攻击者必须花费时间寻找方法进入它们。通过使用检测和响应过程可以实现数据资料和系统的保护。关键的问题是要协调 IDS 系统，事件响应过程要很好的定义。DMZ 也可以限制内部对外部网和 Internet 的访问。DMZ 限制了来自 DMZ 主机的对外访问，增加了内部系统的安全性，阻止了入侵者把网络作为工具对其他人进行攻击。如果 DMZ 仅允许有效的向外的通信量，系统作为攻击的第三方的机会将大大减少。意识到 DMZ 好处的关键是理解它仅是广义上的深度防御的一部分。通过入侵检测系统和基于主机的安全措施可以增加 DMZ 的价值。控制和监测技术的结合体可以很大程度上减少那些对数据提供广泛访问的系统的安全性。

系统安全的根本目标是数据资料的安全，而数据资料是由它的使用者进行存取和维护的。传统的数据存取和维护，都是以新的数据覆盖旧的数据，对于数据的无心错误，或有心的更改数据，一个管理者并无法有效地查出蛛丝马迹。因此，对数据的存取控制是系统安全的一个重要方面。为此，Sandhu 等学者提出了一套以角色为基础的存取控制理论，其基本组件包括使用者、角色、授权及会话。最小特权原则是系统安全中最基本的原则之一。所谓最小特权，指的是在完成某种操作时所赋予网络中每个主体（用户或进程）必不可少的特权。最小特权原则则是指应限定网络中每个主体所必须的最小特权，确保可能的事故、错误、网络部件的篡改等原因造成的损失最小。最小特权原则一方面给予主体必不可少的特权，这就保证了所有的主体都能在所赋予的特权之下完成所需要完成的任务或操作；另一方面，它只给予主体必不可少的特权，这就限制了每个主体所能进行的操作。最小特权原则要求每个用户和程序在操作时应当使用尽可能少的特权，而角色允许主体以参与某特定工作所需要的最小特权去签入系统。被授权拥有强力角色的主体，不需要动辄运用到其所有的特权，只有在那些特权有实际需求时，主体才去运用它们。如此一来，将可减少由于不注意的错误或是侵入者假装合法主体所造成的损坏发生，限制了事故、错误或攻击带来的危害。它还减少了特权程序之间潜在的相互作用，从而使对特权无意的、没必要的或不适当的使用不太可能发生。这种想法还可以引申到程序内部：只有程序中需要那些特权的最小部分才拥有特权。

4.13.2　物理安全

1．保证机房环境安全

信息系统中的计算机硬件、网络设备及其运行环境是信息系统运行的最基本因素，其安全性对信息系统的安全有着十分重要的作用。物理安全是指在物理介质层次上对存储和传输的网络信息进行安全保护，是网络信息安全的基本保障。物理安全包括物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水防潮、防静电、温湿度控制、电力供应和电磁防护等方面的内容。物理安全是指在物理介质层次上对存储和传输的网络信息进行安全保护，是网络信息安全的基本保障。建立物理安全体系结构应从三个方面考虑：一是自然灾害、物理损坏和设备故障；二是电磁辐射、乘机而入、痕迹泄漏等；三是操作失误、意外疏漏等。物理网络的基础设施包括物理介质的选择和网络拓扑结构。物理安全控制是对物理基础设施、物理设备安全和物理访问的控制。对于现有的网络，如果为了适应已经改变的环境而正在创建或修改安全策略，就有必要更改物理基础设施，改变某些关键设备的物理位置，使安全策略更容易实施。如果已经将物理安全控制与安全策略相结合，那么当企业需要扩充和增加新的站点时，就应该在创建站点的同时考虑网络的物理安全控制。受限区域的物理访问需要主要根据分析或物理安全调查的结果来决定，严格限制接近机柜和关键网络基础设施设备所在地，除非经过授权或因工作需要，否则将禁止接近这些区域。设备问题可能会造成严重危害，当采用机柜放置所有关键的网络基础设施设备时，必须尽量使机柜处于一个独立的区域。当打印机密的配置文件或发送含配置内容的传真时，为了避免打印机或传真机的打印输出落入他人手中，需要将敏感打印机和传真机安装在 LAN 网段上，且该局域网应位于访问受到严格控制的室内。除此之外，还必须采取安全的方法来销毁打印输出和文档，如使用碎纸机。为保护关键的网络资源，必须安装和实施充分的环境安全保护。环境安全保护包括：水灾的预防、监测和恢复；水害预防、监测和恢复；电源保护；温度控制；湿度控制；保护免受自然灾害的侵袭，包括地震、闪电和风暴等；保护不受过量磁场干扰；制定良好的清洁制度，减少尘土和垃圾。

2．选用合适的传输介质

屏蔽式双绞线的抗干扰能力更强，且要求必须配有支持屏蔽功能的连接器件和要求介质有良好的接地（最好多处接地）。对于干扰严重的区域，应使用屏蔽式双绞线并将其放在金属管内以增强抗干扰能力。

光纤是超长距离和高容量传输系统最有效的途径，从传输特性等分析，无论何种光纤，都有传输频带宽，速率高、传输损耗低，传输距离远、抗雷电和电磁的干扰性好、保密性好，不易被窃听或截获数据、传输的误码率很低，可靠性高、体积小和重量轻等特点。与双绞线或同轴电缆不同的是，光纤不辐射能量，能够有效地阻止窃听。

3．保证供电安全可靠

计算机和网络主干设备对交流电源的质量要求十分严格，对交流电的电压和频率，对电源波形的正弦性，对三相电源的对称性，对供电的连续性、可靠性、稳定性和抗干扰性等各项指标都要求保持在允许偏差范围内。机房的供配电系统设计既要满足设备自身运转的要求，又要满足网络应用的要求，必须做到保证网络系统运行的可靠性，保证设备的设计寿命，保证信息安全，保证机房人员的工作环境。机房的供配电应满足《电子计算机场地通用规范》GB/T2778-2000 的规定，其供配电系统的电源频率为 50Hz，电压为 220V 或 380V，需要提供的电源相数为三相五线或三相四线制，单相为单相三线制。供配电系统容量应该按照机房所配备设备情况确定，同时考虑系统扩展、升级的可能，预留备用容量。计算机网络机房的负荷等级应该设为一级负荷，供配电系统应该按照一类供电方式设计，即为提高机房设备的供配电系统可靠性，在配电设备前端增加交流不间断电源系统 UPS，达到供电可靠不间断，质量稳定无干扰。

计算机网络机房供配电系统应该是一个独立的系统，通常由计算机网络设备供电、机房辅助设备供电和其他供电三部分组成。计算机网络设备供电部分负责向网络主干通信设备、网络服务器设备、计算机终端设备和计算机外部设备供电；机房辅助设备供电部分负责向机房空调通风系统、机房照明系统和机房维修电源系统（活动地板下或墙面专用电源插座系统）供电；办公室属于其他部分供电。这些部分都统一通过安装在机房配电间的动力配电柜进行配电。外部供电电缆先进入机房总配电柜，然后分送各个部分。机房动力配电柜应该选用自动的空气开关，并且与消防系统联动。当机房出现严重事故或者火警时，管理人员能够立即切断所有电源。在与公共电网的配接方面，有条件的机构最好采用双路电源供电，即接入计算机网络机房的总进线有两路，且来自不同的供电单位。两路供电在总配电系统中可以自动进行切换。当一路供电发生故障时，能够自动转换到另一路。必要时配置防浪涌抑制器。电网中过高或过频的高能瞬态浪涌的侵入，轻者会造成计算机设备的误码率增大，重者会造成设备损坏。因此，根据情况可以在电源输入端配置防浪涌抑制器。机房对电网供电质量要求较高，内容主要包括稳态电压偏移范围、稳态频率偏移范围、电压波形畸变率、允许断电持续时间和三相电压不平衡度等几个主要因素。

对于机房供配电设备，专用配电箱内保护和控制电器的选型应满足国家规范要求，专用配电箱应有充足的备用回路，以满足计算机网络系统设备的扩容；专用配电箱应该设置电流、电压表供管理人员监测三相不平衡情况；专用配电箱要设置足够的中线和接地端子。在机房供配电系统布线方面，机房电源进线应遵照《建筑物防雷设计规范》要求，采取过电压保护措施。专用配电箱电源应采用电缆进线。在不得不采用架空进线时，在低压架空电源进线处或专用电力变压器低压配电母线处，要安装低压避雷器。机房低压配电线路应采用铜芯屏蔽导线或铜芯屏蔽电缆。机房活动地板下的电源线应尽可能地远离网络信号线，避免并排敷设，并采取相应的屏蔽措施。机房内的电线电缆除了应该

具备相应的流量负载承担能力外，还必须考虑线缆阻燃要求。机房内所有电缆的镀锌金属走线槽或镀锌走线钢管都应该布设在地板下面或吊顶内。每路电缆两端都应该进行标记，并且绘制详细的布线图存档。机房的接地系统包括交直流接地、防雷接地、安全保护接地和静电排放接地等多个方面。通常与机房供配电系统或整个建筑物接地系统一同实施，完成后对机房布线提供连接点。机房接地主要有系统接地和屏蔽接地两类。系统接地包括如下 4 种接地类型。

（1）交流工作接地，也称为中性线接地，接地电阻不应大于 4 Ω。

（2）安全保护接地，接地电阻不应大于 4 Ω。

（3）直流工作接地，也称为逻辑接地，通常要求接地电阻不大于 1 Ω。

（4）防雷接地，按照现行的《建筑物防雷设计规范》GB50057-94 设计。屏蔽接地是指对机房辅助设施的静电屏蔽保护层接地，这些静电屏蔽层有线路屏蔽罩、设备外壳、专用供电变压器的静电屏蔽层和局部空间屏蔽罩等。机房接地系统最好采用单点接地，并采取多个设备接地系统经铜排网最后接至同一接地干线的等电位措施。另外，在接线施工中应该尽可能降低中性线对地线的电位。

4.13.3　主机系统安全

主机系统安全主要包括操作系统安全、数据库系统安全、系统访问控制安全、安全审计和主机运行安全。操作系统是重要的系统软件之一，能够对计算机的硬件资源和软件资源实行统一的管理和控制，必须提供必要的手段防止由用户的误操作或者攻击者的人为破坏而造成的错误。操作系统的安全问题主要有两个方面：一是能够为用户提供的安全保护措施，对使用操作系统的用户实施监督，对受保护的对象进行访问控制，采取隔离措施将不同的进程相互隔离开；另一个方面是如何设计和实现一个安全的操作系统，安全的操作系统必须具备最小特权、经济性、开放系统、完全协调、以许可为基础、特权分离、最少公用机构和易使用性等特性。数据库的安全问题主要是存储上的安全问题，保护数据防止不合法的使用，避免数据的泄露、更改和破坏，同时又要为合法地使用提供最大限度的保证。安全的数据库系统应该保证物理数据库和逻辑数据库的完整性和数据的准确性，能够对数据库的访问操作进行跟踪，保证用户仅访问那些允许他访问的数据，同时保证对不同的用户限制使用不同的访问模式，不允许一个未经授权的用户对数据库进行操作，而且能够最大限度地访问允许他访问的数据。主机系统安全主要包括身份鉴别、自主访问控制、强制访问控制、安全审计、系统保护、剩余信息保护、入侵防范、恶意代码防范和资源控制。

操作系统和数据库系统用户的身份标识应具有唯一性，应对登录操作系统和数据库系统的用户进行身份标识和鉴别，对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。操作系统和数据库系统用户的身份鉴别信息应具有不易被冒用的特点，例如口令长度、复杂性和定期更新等。应具有登录失败处理功能，如结束会话、限制非

法登录次数，当登录连接超时自动退出，应具有鉴别警示功能，重要的主机系统应对与之相连的服务器或终端设备进行身份标识和鉴别。

对系统的访问控制分为自主访问控制和强制访问控制。依据安全策略控制主体对客体的访问，对于重要信息资源和访问重要信息资源的所有主体设置敏感标记。自主访问控制的覆盖范围包括与信息安全直接相关的主体、客体及它们之间的操作，自主访问控制的粒度应达到主体为用户级，客体为文件、数据库表级。应由授权主体设置对客体访问和操作的权限，权限分离应采用最小授权原则，分别授予不同用户各自为完成自己承担任务所需的最小权限，并在他们之间形成相互制约的关系，实现操作系统和数据库系统特权用户的权限分离，严格限制默认用户的访问权限。强制访问控制的覆盖范围应包括与重要信息资源直接相关的所有主体、客体及它们之间的操作，强制访问控制的粒度应达到主体为用户级，客体为文件、数据库表级。

安全审计应覆盖到服务器和客户端上的每个操作系统用户和数据库用户，安全审计应记录系统内重要的安全相关事件，包括重要用户行为、系统资源的异常使用和重要系统命令的使用，安全相关事件的记录应包括日期和时间、类型、主体标识、客体标识和事件的结果等，安全审计应可以根据记录数据进行分析，并生成审计报表。安全审计可以对特定事件提供指定方式的实时报警，审计进程应受到保护，避免受到未预期的中断；审计记录应受到保护，避免受到未预期的删除、修改或覆盖等。系统因故障或其他原因中断后，应能够以手动或自动方式恢复运行。保证操作系统和数据库管理系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中，应确保系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

进行主机运行监视，包括监视主机的CPU、硬盘、内存和网络等资源的使用情况，设定资源报警阈值，以便在资源使用超过规定数值时发出报警。进行特定进程监控，限制操作人员运行非法进程。进行主机账户监控，限制对重要账户的添加和更改，检测各种已知的入侵行为，记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。能够检测重要程序完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。服务器和终端设备（包括移动设备）均安装实时检测和查杀恶意代码的软件产品，主机系统防恶意代码产品具有与网络防恶意代码产品不同的恶意代码库，能够支持恶意代码防范的统一管理。限制单个用户的多重并发会话，并且对最大并发会话连接数和一个时间段内可能的并发会话连接数进行限制，通过设定终端接入方式、网络地址范围等条件限制终端登录。根据安全策略设置登录终端的操作超时锁定和鉴别失败锁定，并规定解锁或终止方式，禁止同一用户账号在同一时间内并发登录，限制单个用户对系统资源的最大或最小使用限度。当系统的服务水平降低到预先规定的最小值时，能够检测和报警，根据安全策略设定主体的服务优先级，根据优先级分配系统资源，保证优先级低的主体处理能力不会影响到优先级高的主体的处理能力。

4.14　安全审计

4.14.1　安全审计的内容

4.14.1.1　安全审计概述

安全审计包括识别、记录、存储、分析与安全相关行为的信息，审计记录用于检查与安全相关的活动和负责人。美国国家标准《可信计算机系统评估准则》对于安全审计系统给出如下定义：一个安全的审计系统，是对系统中任何一个或者所有安全相关的事件进行记录、分析和再现的处理系统，通过对一些重要的事件进行的记录在系统发现错误或者受到攻击时能够定位错误和找到攻击成功的原因，是事故后调查取证的基础。在信息安全的三个基本要素——保护、检测和恢复中，安全属于检测的范围。安全审计是指将系统的各种安全机制和措施与预定的安全目标和策略进行一致性比较，确定各项控制机制是否存在和得到执行，对漏洞的防范是否有效，评价系统安全机制的可依赖程度。从广义上来说，安全审计是对网络的脆弱性进行测试评估和分析，最大限度地保障业务的安全正常运行的一切行为和手段。目前已被广泛地用于评估一个系统的安全性的 CC 标准对于网络安全审计定义了一套完整的功能，内容包括安全审计自动响应、安全审计数据生成、安全审计分析、安全审计浏览、安全审计事件存储和安全审计事件选择等。

1）安全审计自动响应（AU_APR）

安全审计自动响应定义在被测事件指示出一个潜在的安全攻击时做出的响应，它是管理审计事件的需要，这些需要包括报警或行动，例如包括实时报警的生成、违例进程的终止、中断服务和用户账号的失效等。根据审计事件的不同，系统将做出不同的响应。其响应方式可作增加、删除和修改等操作。

2）安全审计数据生成（AU_GEN）

该功能要求记录与安全相关的事件的出现，包括鉴别审计层次、列举可被审计的事件类型以及鉴别由各种审计记录类型提供的相关审计信息的最小集合。系统可定义可审计事件清单，每个可审计事件对应于某个事件级别，如低级、中级、高级。产生的审计数据有以下几方面。

（1）对于敏感数据项（如口令等）的访问。

（2）目标对象的删除。

（3）访问权限或能力的授予和废除。

（4）改变主体或目标的安全属性。

（5）标识定义和用户授权认证功能的使用。

（6）审计功能的启动和关闭。

每一条审计记录中至少应所含以下信息：事件发生的日期、时间、事件类型、主题标识、执行结果（成功、失败）、引起此事件的用户的标识以及对每一个审计事件与该事件有关的审计信息。

3）安全审计分析（AU_SAA）

此部分功能定义了分析系统活动和审计数据来寻找可能的或真正的安全违规操作。它可以用于入侵检测或对安全违规的自动响应。当一个审计事件集出现或累计出现一定次数时可以确定一个违规的发生，并执行审计分析。事件的集合能够由经授权的用户进行增加、修改或删除等操作。审计分析分为潜在攻击分析、基于模板的异常检测、简单攻击试探和复杂攻击试探等几种类型。

（1）潜在攻击分析。系统能用一系列的规则监控审计事件，并根据规则指示系统的潜在攻击。

（2）基于模板的异常检测。检测系统不同等级用户的行动记录，当用户的活动等级超过其限定的登记时，应指示出此为一个潜在的攻击。

（3）简单攻击试探。当发现一个系统事件与一个表示对系统潜在攻击的签名事件匹配时，应指示出此为一个潜在的攻击。

（4）复杂攻击试探。当发现一个系统事件或事迹序列与一个表示对系统潜在攻击的签名事件匹配时，应指示出此为一个潜在的攻击。

4）安全审计浏览（AU_SAR）

该功能要求审计系统能够使授权的用户有效地浏览审计数据。包括审计浏览、有限审计浏览和可选审计浏览。

（1）审计浏览。提供从审计记录中读取信息的服务。

（2）有限审计浏览。要求除注册用户外，其他用户不能读取信息。

（3）可选审计信息。要求审计浏览工具根据相应的判断标准选择需浏览的审计数据。

5）安全审计事件选择（AU_SEL）

系统能够维护、检查或修改审计事件的集合，能够选择对哪些安全属性进行审计，例如，与目标标识、用户标识、主体标识、主机标识或事件类型有关的属性。系统管理员将能够有选择地在个人识别的基础上审计任何一个用户或多个用户的动作。

6）安全审计事件存储（AU_STG）

系统将提供控制措施以防止由于资源的不可用丢失审计数据。能够创造、维护、访问它所保护的对象的审计踪迹，并保护其不被修改、非授权访问或破坏。审计数据将受到保护直至授权用户对它进行访问。它可保证某个指定量度的审计记录被维护，并不受以下事件的影响。

（1）审计存储用尽。

（2）审计存储故障。

（3）非法攻击。

（4）其他任何非预期事件。

系统能够在审计存储发生故障时采取相应的动作，能够在审计存储即将用尽时采取相应的动作。

信息安全的目标分为系统安全、数据安全和事务安全，根据被审计对象的不同，安全审计包含以下几种类型。

（1）系统的安全审计。

（2）数据的安全审计。

（3）应用的安全审计。

但是，通常的审计系统都含有上述三种审计目的。审计系统必须支持各种操作系统（如 UNIX/Linux/Windows）、网络设备（多种网络交换机、路由器）、支持服务和应用系统（如 IIS 服务器、APAEHE 服务器、Web 服务器、E-mail 服务器、FTP 服务器和 DNS 服务器等）、支持新设备和系统日志的审计。

4.14.1.2 安全审计的功能

安全审计系统就是根据一定的安全策略记录和分析历史操作事件及数据，发现能够改进系统运行性能和系统安全的地方。安全审计的作用包括对潜在的攻击者起到震慑或警告的作用、检测和制止对安全系统的入侵、发现计算机的滥用情况、为系统管理员提供系统运行的日志，从而能发现系统入侵行为和潜在的漏洞及对已经发生的系统攻击行为提供有效的追纠证据。安全审计系统通常有一个统一的集中管理平台，支持集中管理，并支持对日志代理、安全审计中心、日志、数据库的集中管理，并具有事件响应机制和联动机制。中国安全产品测评认证中心基于 CC 标准来制定国家标准，网络安全审计系统所实现的功能主要遵照 CC 标准。功能如下。

1）监视网络上的反常行为

此功能对应于 CC 标准的安全审计分析功能和安全审计数据生成功能。基于网络的审计代理以旁路（by-pass）方式连接在被审计的网络上，实时监测网络上的传输内容，根据规则分析，辨别出异常行为，如系统入侵、攻击尝试、内部违规和非法访问等行为。它不但能够检测到外来入侵，也能发现内部人员的违规或误操作。审计系统能够通过分析系统活动和审计数据来确认安全违规操作。当一个审计事件集出现或累计出现一定次数时可以确定一个违规的发生，并对此事件集进行分析。授权的用户能够对事件集合进行增加、修改或删除等操作。

2）收集操作系统和应用系统内部所产生的审计数据

此功能对应于 CC 标准的安全审计分析功能和安全审计数据生成功能。基于主机的审计代理嵌入在被审计主机系统内部，收集操作系统或应用系统所产生的审计信息，如系统日志、报警消息和操作记录等。该功能主要防止操作系统或应用系统的日志文件或相关信息被黑客删除或意外丢失而带来的损失，是一种取证功能。

3）实时报警

此功能对应于 CC 标准的安全审计自动响应功能。当审计系统检测到网络违规行为或异常情况时进行实时报警，以提醒管理人员及时发现问题，并采取有效措施控制事态发展。系统是根据不同事件级别产生不同级别的报警，如不同的报警声音或不同的记录形式。

4）网络控制

此功能对应于 CC 标准的安全审计自动响应功能。当审计系统发现严重的违规现象或网络入侵时，可通过自动或手动的方式中断此网络连接，使入侵不能继续进行，能有效地减少损失，维护网络秩序，保证网络安全。

5）审计数据维护和查询加密，权限控制

此功能对应于 CC 标准的安全审计数据生成、安全审计复查和安全审计事件存储功能。所有触发审计系统的事件都在审计系统内按照 CC 标准生成完备的审计数据，并加密存储在审计系统内，同时能够根据存储的记录和操作者的权限进行查询、统计、管理和维护等操作。并且能够在必要时从记录中抽取所需要的资料，例如：

（1）一个或多个用户的行动。

（2）对一个特定目标或资源采取的行动。

（3）审计例外的情况。

（4）与特定安全属性有关的行动。

审计系统能够提供控制措施以防止丢失审计数据。能够创造、维护、访问它所保护的对象的审计记录，并保护其不被修改、非授权访问或破坏。

6）规则制定

此功能对应于 CC 标准的安全审计事件选择功能。系统根据管理员所制定的规则来运作，以适应不同应用的需求，使得审计系统与信息系统更加贴切。在审计系统中能定义可审计的事件清单，每个可审计事件对应于某个事件级别，如低级、中级、高级。产生的审计数据有以下几方面。

（1）对于敏感数据项（如口令等）的访问。

（2）目标对象的删除。

（3）访问权限或能力的授予和废除。

（4）改变主体或目标的安全属性。

（5）标识定义和用户授权认证功能的使用。

每一条审计记录中包含以下信息：事件发生的日期、时间、事件类型、主题标识、执行结果（成功、失败）、引起此事件的用户的标识以及对每一个审计事件与该事件有关的审计信息等。

7）附加功能

除了提供以上符合 CC 标准的功能之外，审计系统还提供审计接口，能够与其他安

全产品协同工作，联合防御。

4.14.1.3　安全审计模型

在安全审计模型中，当检测出一个事件后，必须做出决定该事件是安全相关事件还是与安全无关的事件。事件鉴别器接收到事件后，确定应该产生安全审计消息，或者产生安全报警消息，或者两者都产生。安全审计消息发送到审计记录器，安全报警发送到报警记录器，等待下一步的评估和行动。安全审计消息被格式化，转换成安全审计记录，包括在安全审计跟踪里。部分安全审计跟踪可能存档，安全审计跟踪和安全审计跟踪的存档都用来产生安全报告，这些报告的来源是针对特别的标准选择特别的安全审计跟踪记录。总之，安全审计跟踪可能用于分析，安全审计报告或者安全报警的产生，其模型如图 4-133 所示。

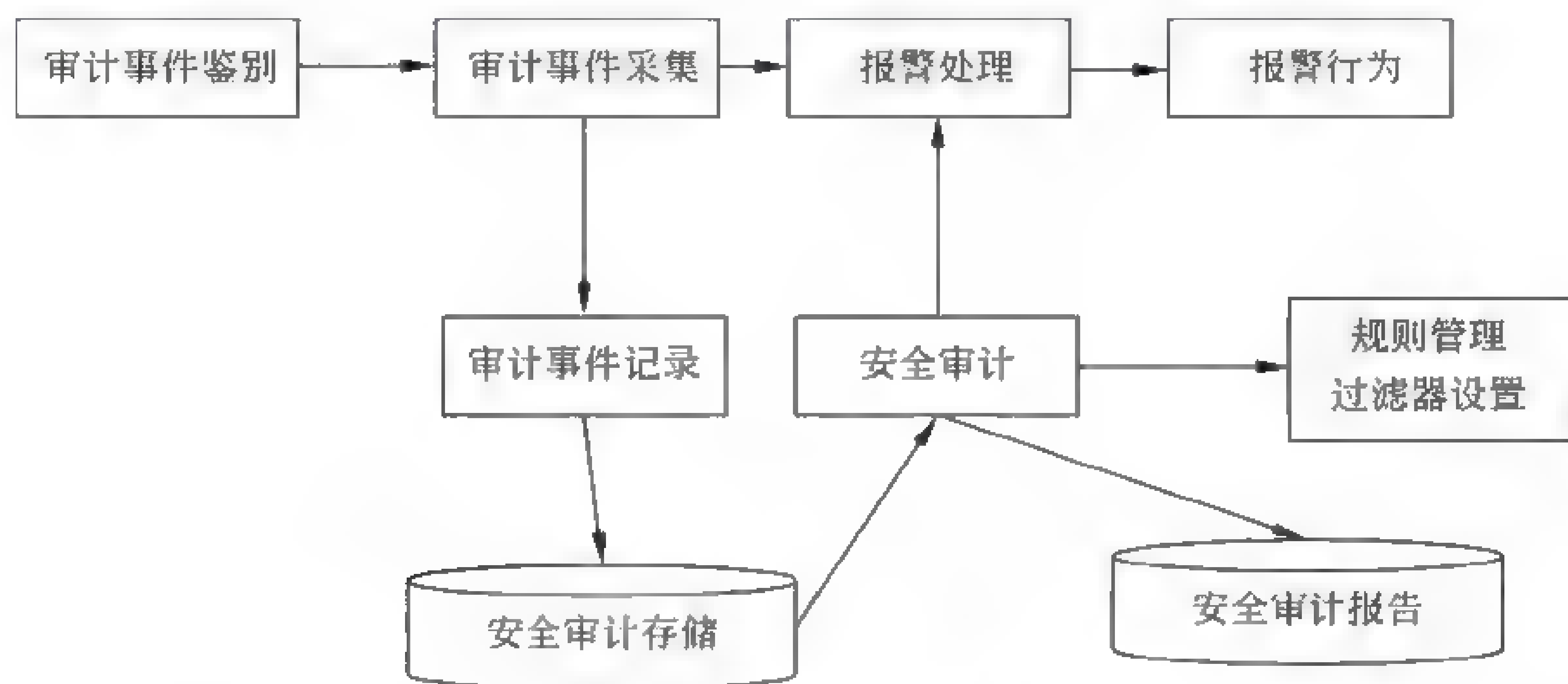


图 4-133　安全审计模型

安全审计规则管理为保证系统在有安全保障的条件下有效运行，为审计管理员提供了详细的规则管理，包括对来访 IP 的过滤，对特定注册用户的过滤，对恶意刷新可自定义设置次数/秒数的屏蔽，以及对数据库审计的各种接口的管理。

安全审计事件鉴别在实施审计过滤体系前对审计事件进行鉴别，以确定哪些事件需要重点审计，据此来配置相应的过滤器链，开发相应的审计事件的记录组件等。安全审计日志采集完成了安全审计的核心功能，实现了在线日志采集和离线日志采集。在线日志通过访问者的 SessionID 可以得到用户访问的序列，而离线日志则会触发过滤器组件或者数据库层触发器，存储审计日志于数据库中。

安全审计日志采用数据库存储，主要包括用户的访问日志和数据库审计视图。其中，用户的访问日志主要包括会话标识符、用户名、IP 地址和资源等主要信息；数据库审计视图是数据库系统的一个特性，通过具体审计策略的定义，可以得到相关实体操作、权限操作的记录，以供审计使用。

安全审计报告要为管理员提供各种查询统计的接口，以做到有效的追踪，对具体操作的有据可考。具体包括对各类别日志的自定义模糊查询、提取高频率信息流、对大量访问日志的细度分析及对海量日志的转储方案等。

安全审计报警处理及报警行为对于违规访问及恶意刷新，系统会进行报警处理，自动提取来访或用户名，将其置入危险库或者拒绝服务用户库，再次的访问将被服务器拒绝。

同时，日志作为安全审计系统得到的核心数据，考虑其安全性也是十分必要的，项目中通过数据库系统设置和文件过滤器的配合，来控制对日志物理文件的访问，以确保日志文件不被非授权访问和篡改。

4.14.1.4 安全审计的流程

电子数据安全审计工作的流程是：收集来自内核和核外的事件，根据相应的审计条件判断是否是审计事件。对审计事件的内容按日志的模式记录到审计日志中。当审计事件满足报警阈值时，则向审计人员发送报警信息并记录其内容。当事件在一定时间内连续发生，满足逐出系统阈值，则将引起该事件的用户逐出系统并记录其内容。

安全审计过程如下。

（1）记录和搜集有关的审计信息，产生审计数据记录。

（2）对数据记录进行安全违反分析，以检查安全违反与安全入侵原因。

（3）对其分析产生相应的分析报表。

（4）评估系统安全，并提出改进意见。

其简化为三个功能模块，如图 4-134 所示。

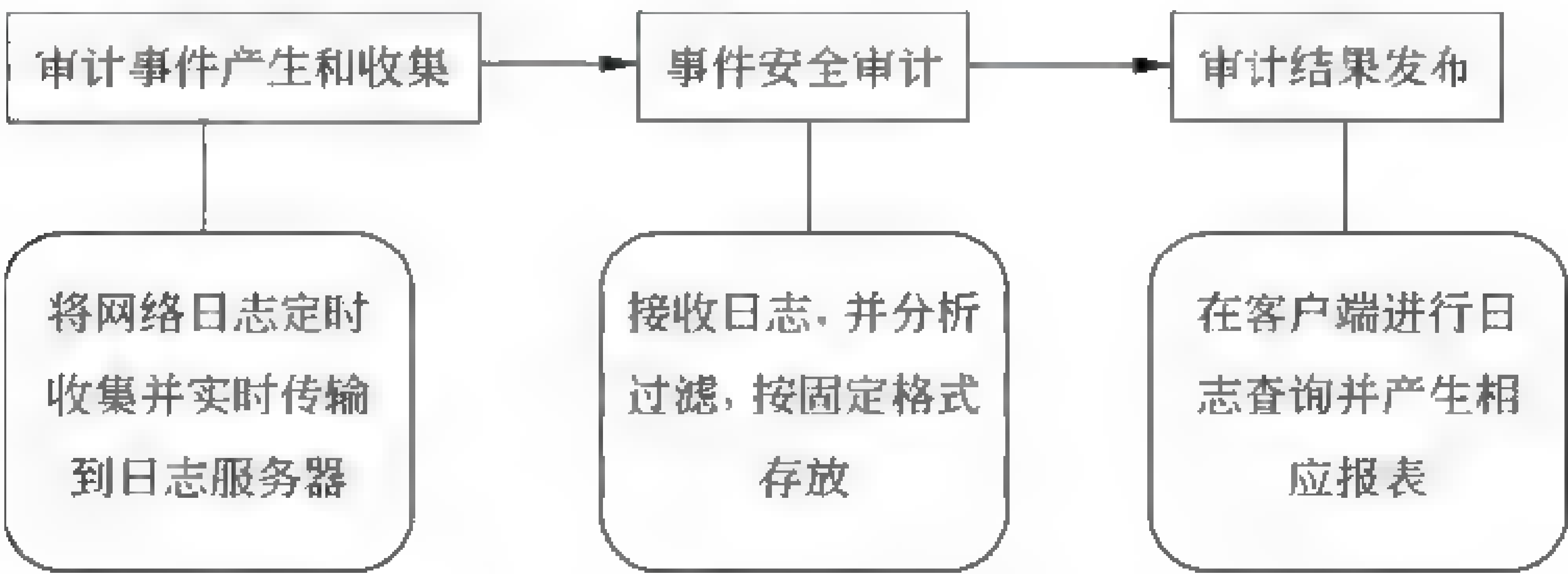


图 4-134 安全审计流程

常用的报警类型有用于实时报告用户试探进入系统的登录失败报警以及用于实时报告系统中病毒活动情况的病毒报警等。审计人员可以查询、检查审计日志以形成审计报告。检查的内容包括审计事件类型、事件安全级、引用事件的用户、报警、指定时间内的事件以及恶意用户表等，上述内容可结合使用。

基于主机的安全审计是对每个用户在计算机系统上的操作做一个完整的记录，主要

包括系统启动、运行情况、管理员登录、操作情况、系统配置更改（如注册表、配置文件和用户系统等）以及病毒或蠕虫感染、资源消耗情况的审计，硬盘、CPU、内存、网络负载、进程、操作系统安全日志、系统内部事件、对重要文件的访问记录，便于发现、调查、分析以及事后追查责任。一般来说，安全审计过程的实现分为三步：收集审计事件；产生审计日志记录；根据记录进行安全分析、生成报警信息。审计范围包括操作系统和各应用程序，其中，操作系统的审计主要是检测和判定对系统的渗透和识别误操作、文件操作和操作命令的选择、文件的定义和自动转换、文件系统完整性的定时检测、信息的格式和输出媒体的格式、报警阈值的选择和设置、审计日志记录及其数据的安全保护等。各应用程序的审计主要是针对应用程序的某些操作作为审计对象进行监视和实时记录，并且根据记录结果判断此应用程序是否被修改、安全控制和正确运行，判断程序和数据是否完整，依靠使用者的身份、口令验证和终端保护等方法控制应用程序的正确运行。审计有人工审计，计算机手动分析、处理审计记录并与审计人员最后决策相结合的半自动审计，依靠专家系统做出判断结果的自动化的智能审计等。为了支持审计工作，要求数据库管理系统具有高可靠性和高完整性。数据库管理系统要为审计的需要设置相应的特性。

4.14.1.5　基于网络的安全审计系统

网络安全审计是一个安全的网络必须支持的功能特性。审计是记录用户使用计算机网络系统进行所有活动的过程，它不仅能够识别谁访问了系统，还能指出系统正被怎样地使用，对于确定是否有网络被攻击的情况以及确定攻击源也很重要。同时，系统事件的记录能够更迅速和系统地识别问题，是网络事故处理的重要依据，能够为网络犯罪行为及泄密行为提供取证基础。另外，通过对安全事件的不断收集、积累并加以分析，可以有选择地对某些主机和用户进行审计跟踪和监控。

从网络管理角度讲，安全审计便是实现内部监督的重要手段。内部网络的管理和安全的程度是因特网成熟的标志。因此，内部的安全监督必不可少，安全审计系统可以有效地实现对内网的安全监督。在我国网络快速发展和应用的过程中，包括政府、学校、企事业单位和军队等在内的办公自动化系统、数字化校园系统、电子商务系统、电子政务和金融网络等系统的规模越来越大，构成系统的网络、计算机系统不同，使用人员和技术水平、安全意识参差不齐，确保信息网络安全已经成为必须要考虑的紧迫问题。

当前，网络安全审计系统的发展相对落后，这和用户的需求形成了鲜明对比。网络安全审计系统重点审计网络访问行为及网络报文（message），就现实情况而言，国内大部分的企业都已经建立起了自己的计算机网络，即企业网（Enterprise Network，通常指 Intranet），但一般都没有建立相应的网络安全审计系统，这一方面是由于缺乏比较好的网络安全审计技术，更重要的一个原因是大家对网络安全审计的认识存在不足，这从我国每年不断发生的网络泄密事件可见一斑。与 Internet 互连的网络安装防火墙、IDS、杀

毒软件可在一定程度上解决网络黑客与病毒入侵等问题，但是对于一个单位的网络来说，仅仅有这样的配置是不够的。一个单位的网络常常既要处理来自外部的入侵，也要对内部用户访问外部网络的行为进行监控，只有这样，一个单位内部网络连接到外部网络时才能是比较安全的。显然，研究并建立一套与实际应用需求相适应的网络安全审计系统具有重要的现实意义。

网络安全审计系统在设计上采用了分布式审计和多层次审计相结合的独特方案。网络安全审计系统是对网络系统多个层次上的全面审计。多层次审计是指整个审计系统不仅能对网络数据通信操作进行底层审计（如网络上的各种 Internet 应用），还能对系统和平台（包括操作系统和应用平台）进行中层审计，以及为应用软件服务提供高层审计。这使它区别于传统的审计产品和 IDS 系统。

同时，对于一个地点分散，主机众多，各种联网方式共存的大规模网络，网络安全审计系统应该覆盖整个系统，即网络安全审计系统应对每个子系统都能进行安全审计，这样才能保证整体的安全。因此，网络安全审计系统除了是一个多层次审计系统之外，还是一个分布式的审计系统。网络安全审计系统由各种特定类型的审计代理（audit agent）、审计收发器（audit transceiver）、审计中心（audit center）和审计控制台（audit console）4 部分组成。审计代理安置在所有被监视的网络节点以及关键的主机节点，进行审计数据的收集、审计数据的分析、审计事件的上报和审计事件的实时反应等工作。审计收发器负责收集该主机上所有审计代理产生的审计事件，将审计事件上报审计中心或将审计事件在整个审计域中相关的审计代理间广播；同时根据审计中心或审计控制台发出的审计指令对该主机上的审计组件进行控制，如更新配置、重启和自检等。审计中心则完成审计事件的分析、统计和存储等。审计控制台提供图形化的用户接口，完成审计事件的实时报警、安全规则的制定、审计组件的控制管理等工作。同时，网络安全审计系统还提供了审计接口。审计接口为其他网络安全设备及各种应用程序提供了进行审计的手段。其他网络安全产品如防火墙等可通过审计接口与审计组件进行信息交换，使得审计系统能够和其他安全产品进行联合防御，以提高网络安全程度。同时，用户所开发的应用程序也可以通过审计接口使得应用程序能够被审计系统进行审计，以保护应用程序不受侵害。

各组件的关系描述如下。

（1）网络安全审计系统可以分布在任意多个主机上，每个主机上可以有任意多个审计代理。

（2）在同一主机上的所有审计代理向位于该主机上的审计收发器发送信息。

（3）每台主机只能有一个收发器，负责监督和控制该主机上的所有代理，可以向代理发送控制命令，也可以对代理所发送来的数据进行数据精简。

（4）审计收发器向审计中心报告审计事件。

（5）审计中心监督和控制所有的审计发送器。

（6）审计控制台负责同用户进行交互，对整个审计系统进行管理，从用户界面获取控制命令，向用户实时报警等。

（7）所有部件都为其他部件及用户提供 API，实现相互之间的调用。

网络安全审计系统的各部分具体功能如下。

1）审计代理

整个审计体系的基础由分布在审计节点上的审计代理构成。这些审计代理是独立运行的软件或模块，根据不同的需求安装在不同的系统中，完成不同的功能。这些代理通过网络旁路接入和系统嵌入的方式与实际运行的系统连接，采用被动或主动的方式获取信息，根据事先定义好的安全策略进行分析，生成审计事件，上报审计中心，并且在某些情况下还将作用于实际运行系统配合响应机制的完成。主要功能如下。

（1）审计数据生成。

（2）分析审计数据，生成审计事件。

（3）审计事件的记录和跟踪。

（4）安全事件的实时报警。

（5）及时对网络及设备进行控制，消除安全威胁。

产生审计事件的因素如下。

（1）身份认证机构不能确认的身份。

（2）访问安全等级不相符合的数据。

（3）对系统运行产生重要影响的动作。

（4）其他与安全相关的动作。

每一条审计事件中包含以下信息：事件发生的日期、时间、事件类型、主题标识、执行结果（成功、失败）、引起此事件的用户的标识以及对每一个审计事件与该事件有关的审计信息。

这些审计代理大致分为 4 类。

- 网络监听式审计代理：安装在专用审计硬件系统上，或者通用 PC Server 的 NT 操作系统上，通过对网络上传输的数据包进行截获和分析的方式运行。例如，入侵检测审计代理、流量监控审计代理、典型应用审计代理、文件共享审计代理和网管操作审计代理。
- 主机操作系统审计代理：安装在服务器上，嵌入在 UNIX 或者 NT 操作系统中，通过收集操作系统日志和内部安全事件的方式运行。例如，NT 操作系统审计代理、Solaris 操作系统审计代理和 HP_UX 操作系统审计代理。
- 主动获取式审计代理：通过主动向预定的目标以标准格式发送请求，接收回应，然后判断的方式运行。例如，网络设备 MIB 采样审计代理、漏洞扫描审计代理。
- 应用型审计代理：本身是一个应用，但能够向审计中心发送审计事件，进行报警或通报日常数据。例如，文件完整性审计代理等。

审计代理同时也具有很强的自治性。其自治性主要体现在它们是独立运行的实体，可以将它们看成是一个独立的进程或进程组，它们的执行只与操作系统的调度有关，而与其他进程无关。尽管代理间可能需要进行数据通信，但仍认为它是自治的。自治代理的引入可以改善网络安全审计系统的健壮性和可扩展性。由于代理是相互独立运行的实体，它们的运行和删除不会影响到其他组件的运行，使得整个系统不用重启。可以根据系统的需要，灵活地增加任意多的代理和开发新的针对特定应用的代理，只要它们符合审计系统各组件间的逻辑关系并以同样的审计协议进行数据通信。

2）审计收发器

审计收发器作为该主机上的审计代理与审计域中其他的审计组件进行通信的中介。主要功能如下。

（1）收集该主机上所有审计代理产生的审计事件。

（2）将审计事件上报审计中心。

（3）将审计事件在相关审计代理间广播。

（4）对该主机上的审计组件进行控制。

3）审计中心

审计中心收集由审计收发器送来的审计事件，具有分析、统计和存储等功能。

- 分析：分析安全审计事件与系统运行状况。
- 统计：根据审计事件进行统计汇总。
- 存储：对审计事件进行分析后存入相应的数据库。

4）审计控制台

审计系统的图形化用户接口。系统管理员通过该接口对整个安全审计系统进行控制管理，通过它能创造、维护、访问审计系统所保护的对象的审计踪迹，对系统进行配置等。

- 实时报警：安全事件的实时浏览。
- 分级控制：不同级别的用户能对审计系统进行不同程度的控制管理。
- 检索：供系统管理员检索历史的安全事件。
- 审计事件选择：为各个审计代理设置特定的安全策略。
- 审计组件管理：包括组件的配置、存储管理、时钟管理和数据库管理。

4.14.2 审计工具

4.14.2.1 审计工具分类

审计的内容多种多样，为了不同的目的可以采取不同的方法和工具。审计工具按照不同的目的可以分为如下几类。

（1）行为审计。实时监测网络中的应用情况，对用户网络的各种应用行为（网站访问、收发邮件、上传和下载、即时通信、网络游戏和视频等）进行监测、报警、记录和审计；统计网络各种应用流量和用户 IP 流量，了解网络带宽和应用的使用，发现存在的问题，提高网络使用效率。通过丰富的审计数据和统计数据，及时发现异常应用，帮助管理者快速分析定位问题对象。

（2）内容审计。对用户的网络应用内容进行监测审计，可以设定地址、用户名和应用协议等监测条件对应用内容进行审计，也可以设定关键词、组合词和模糊匹配对特定的应用内容（网页、邮件、上传下载、即时通信和聊天的文字内容）进行监测审计。

（3）主机审计。实时对网络中服务器和用户终端的访问与操作进行监测审计，可以掌握每个主机的资源使用情况，监测主机接入的合法性，记录对文件系统的访问操作行为，记录对各外设的操作，监测加载的程序和进程，监控对外部网络的连接和访问。

（4）数据库审计。实时监测对数据库服务器的网络访问行为，对系统操作和数据操作进行记录，监测和报警数据库操作中的越权、敏感或违规行为，审计重要的数据库操作细节。

目前常见的日志审计系统有 LogBase 日志管理综合审计系统、NetSC 日志审计系统和 XLog 网络日志审计系统等。常见的网络安全审计工具有 Netlooker、SmartMonitor、Ratproxy 和 S_Audit 等。

4.14.2.2　审计工具简介

1．LogBase

LogBase 日志管理综合审计系统以保障信息系统的稳定安全为出发点，全面获取和收集各类信息日志，通过实时和事后的审计分析，为用户预防和及时发现整个系统各组成部分（网络、服务器、应用、安全设备、终端）的运行故障、敏感操作和安全事件独有的日志专用数据库和动态索引机制，可以满足海量日志信息的集中存储和高速检索，为各类异常事件的追查和恢复提供有效依据。该系统能够审计的日志包括各类网络设备（交换机、路由器）的系统日志、各类 UNIX/Linux 操作系统的系统日志及其他审计信息、Windows 平台事件的日志内容及其他审计信息、各类应用服务的系统和访问日志、各类网络安全设备日志等。

2．NetSC

NetSC 日志审计系统由 LogServer、LogViewer 和 LogAuditer 三个部分组成，具有操作界面简单、直观易用、稳定性好、易维护及易移植等诸多特性，可以为企事业内部局域网和连接 Internet 用户提供一套全面安全的解决方案。该系统能实时地监测网络上和用户系统中发生的与安全相关的事件，并将这些情况真实、详尽而完善地进行记录，在必要时能提供宝贵的数据，并具有防销毁和篡改的功能。同时该系统提供了完善的日志审计功能，可以从不同的角度进行查询和统计，并将结果以不同的方式进行显示。

3．XLog

XLog 网络日志审计系统，可以与路由器、交换机等网络设备共同组网，根据用户要求采集不同类型的网络流量信息，并通过聚合、分析与统计，为网络管理员提供用户行为审计、流量异常监控和网络部署优化的数据基础和决策依据。XLog 支持多种类型网络流量日志的处理，管理员可以依据网络设备的特性、网络拓扑的特点以及日志分析的目标等因素灵活选择日志采集和分析模式，实时记录稍纵即逝的网络流量信息。NAT 日志可以通过 NE 系列路由器、BAS 等设备记录 NAT 转换前的源 IP 地址、源端口，经过 NAT 转换后的源 IP 地址、源端口，以及所访问目的的 IP、目的端口、协议号、开始时间和结束时间等关键信息。FLOW 日志记录了用户访问外部网络的流信息，包括源 IP、目的 IP、源端口、目的端口、流起始时间、结束时间以及出入流量等关键信息。通过 XLog 对 FLOW 日志的分析与统计，可以形成网络使用状况报表，如各部门流量统计、应用使用量统计和应用吞吐量趋势等报表，可以帮助管理员及时掌握网络的运行状态。DIG 日志又称为探针日志，是由探针型采集器直接从交换机的镜像端口、共享式 HUB 或分流器中采集的用户上网信息，并对访问网络的数据流进行分类统计和内容摘要而生成的日志记录。探针型采集器具有良好的适应性，可以应用于不支持 NAT、FLOW 日志生成的网络环境。

基于日志的网络安全审计系统采用了 B/S 结构。HF 防火墙、IDS 入侵监测系统、IPPS 信息保护系统将产生的日志实时地发送给基于日志的网络安全审计系统，基于日志的网络安全审计系统把日志记录存储在数据库，用户可以通过基于日志的网络安全审计系统的用户控制台审计分析日志。基于日志的网络安全审计系统综合审计这三种安全产品产生的日志，能够更有效地审计系统的安全，同时使得这三种安全产品不用处理庞大的日志数据而浪费大量的系统资源。

4．Netlooker

Netlooker 网络信息安全审计系统由网络的行为审计、内容审计、主机审计和数据库审计 4 大功能模块构成，既可以满足高端用户的一体化综合安全审计需求，也可以根据用户的需求定制某一种需求的安全审计。该产品采用 B/S 结构和 RIA 界面设计，具备强大的网络数据实时侦听、协议解析和数据还原分析功能，实现对网络、主机和数据库的访问和使用行为、信息内容的监控审计，可以有效地实现对网络中的各种应用及信息内容的可控监管，防止利用网络泄露党政军的涉密信息和企业内部核心信息；可以预防传播与社会和谐稳定相悖的不良信息，规范上网行为；可以监测统计各种应用流量，为合理地使用网络资源，提高网络效能。

Netlooker 是新一代企业上网监控软件，其强大的功能、优秀的性能、简洁实用的界面决定了其高品质，是业内领先的一款不可多得的上网监控软件。内置具有世界领先水平的内核抓包引擎 Kercap 保证了软件的高稳定性和高效性；优秀的构架设计及模块化设

计保证了软件的高品质；功能强大的内容分析引擎和高效的索引算法保证了软件的高性能；简单易用，功能强大，实用有效。Netlooker 基于网卡物理地址跨网段（任何 VLAN 环境）、跨平台进行网络监控，可以向网络中任何一台机器发送短消息，对网络中机器名和 IP 的改动进行自动报警，及时发现网络中的不良状况。控制 BT、禁止 QQ 等 P2P 的即时通信工具，防止网络带宽被占用，对网络中计算机进行流量控制，合理分配和管理网络带宽，监控所有 HTTP、FTP 文件的上传或者下载（各种上传或者下载方式）。可禁止网页粘贴、论坛留言和 Web 邮件等所有通过 HTTP 协议的网络外发行为，使单位领导不再担心员工利用单位计算机在网上发布不恰当的网络言论，不再担心企业商业秘密或重要文档通过因特网外泄。不仅可对每台计算机的上网流量进行统计查询，而且还可以根据工作需要对它们进行流量控制，带宽控制，控制 BT 下载并报警，防止网络带宽被大量无效占用，使因特网资源真正得到有效合理地分配。可实时记录 MSN、Yahoo!、ICQ 和 QQ 聊天室等即时通信工具的聊天内容，禁止 QQ，并对 QQ 号码以及其聊天过程进行全程记录。网络中机器名和 IP 地址的任何改动都会进行自动报警提示，在线报警信息实时反映网络出现的不良状况，使网络安全危险和隐患能在第一时间发现和解决，管理者还可通过系统向违规者发送短消息以进行警告。在线动态显示当前上网和未上网的机器，使管理者对整个局域网计算机使用状态一目了然。在线动态显示机器上网信息、聊天内容、禁止 QQ 信息、邮件日志、上传下载日志，并可针对某台机器或某组机器的网上行为实现在线实时监控。可对 VIP 机器进行不做任何监控的放行设置,也可对相关网址或端口进行不做任何监控的放行设置。可在任意时间段对任何组和单机建立各种管理规则进行上网管理，操作灵活方便，使管理者能对因特网实现最大限度的个性化管理。基于网络层进行控制，对 IP 地址进行控制管理，可以只允许通过指定的 IP 也可以阻止指定的 IP 段。基于传输层进行控制，对端口进行控制管理，可以只允许通过指定端口，也可以阻止指定的端口范围。通过对不同级别、不同用户分配不同的管理权限，可实现多级别、多用户对系统进行远程操作控制，使整个因特网管理有条有序，层次分明。不仅可禁止所有 HTTP、FTP 文件的上传或者下载（各种上传或者下载方式），而且可针对上传或下载的文件格式进行各种形式的控制，使上传下载的控制管理更加灵活和有针对性。可对通过 SMTP 协议发邮件和通过 POP3 收邮件的收发邮箱进行上网管理，如只能收发到指定的邮箱或指定的邮箱才能收发。完善库管理，程序自带色情反动库、聊天库、游戏库、财经证券库、搜索引擎库、招聘库、电影休闲库、过滤关键词库和自定义网址库 9 大网址库，用户还可以自己管理相应的 9 个自定义网址库，和 9 个系统自带网址库协同工作，完成整个网络监控的过滤工作。完整记录所有机器的上网信息且可进行，包括机器名、源 MAC 地址、源 IP 地址、源端口、目的 MAC 地址、目的 IP 地址、目的端口地址、操作类型、服务类型、协议类型、标题、内容以及时间。可以将机器按 IP 或者 VLAN 分成不同的组进行系统管理，可以增添和删除组。在实时显示每台机器的 IP 地址、机器名和 MAC 地址的基础上，管理员可以将每台机器进行标志名设定以方便对系统进

行统一管理。可统计和查询各组或者每台计算机的上网字节数和整个网络的总流量。可以对单机或者组查询统计其在任意时间段上的具体上网行为和内容。可分别针对 TCP 协议、UDP 协议、ICMP 协议和 IGMP 协议 4 大协议进行网上日志和内容的统计查询。可分别针对 Web 浏览、Web 张贴、文件上传、文件下载、发送邮件、接收邮件、游戏记录、远程登录、QQ 聊天、MSN 聊天、ICQ 聊天、Yahoo 聊天、P2P 信息、报警日志和禁止 QQ 等各种服务类型进行统计查询。方便实用的日志导出功能，使管理员可将监控日志导出做统一存储或分析。所有日志文件不仅可另存为文本文件，而且可另存为 Excel 文件，且都可打印输出。可将整个软件的信息备份导出另存，方便以后安装时不用再设置。

5. SmartMonitor

SmartMonitor 是一款工作于 PC 上的网络信息审计软件，通过和 Vigor 系列路由器的整合，对网络数据进行获取、过滤、分析，从中将用户关心的内容提取出来并还原为具有很好可读性的格式，生成各种报表，供企业管理人员参考。企业管理人员经常遇到以下困扰：上班时间聊天软件使用过多，影响工作效率；滥用带宽进行下载，导致正常应用的拥塞；公司机密通过聊天软件等工具泄漏。SmartMonitor 是针对企业用户经常遇到的这些问题量身定造的，首先要做的，就是解决企业的网络问题。通过对网络信息的审计，SmartMonitor 可以有效地帮助企业管理人员解决由网络应用派生出的各种问题。无论是上网记录、邮件记录还是聊天记录，下载文件，SmartMonitor 都可以分析整理得井井有条，检查起来非常方便。SmartMonitor 不仅仅是为了管理而管理，它同时为企业用户带来了全新的主动管理的理念。传统的管理模式是被动管理，员工总是在被管理人员关注并通知甚至警告之后，才会约束自己的行为，由此容易让员工产生抵触情绪，而且会带来一些管理问题。而 SmartMonitor 针对此情况，通过提供 Top10 排名功能，让员工可以随时自己去查看各种网络应用的 Top10 排名，例如聊天 Top10、下载 Top10 等，当“榜上有名”时，员工看到就会进行自我约束，从而形成一种自我管理的概念。值得一提的是，SmartMonitor 还提供了报表功能，可以随时生成离线报表，发送给相关人员进行查看。主要功能包括网络服务记录分析、聊天软件使用记录（记录每个用户对聊天软件的使用记录，不仅记录聊天数，对于常用的 MSN、ICQ 和 Yahoo Messenger，还可以将聊天内容进行记录还原，在需要时进行查阅）、邮件使用记录（对 POP3、SMTP 接收、发送的邮件进行记录、发件人、收件人信息、邮件标题、正文以及附件，全部都可以保存）、上网记录（统计每个用户的上网情况，记录访问过的所有网页记录，可以轻松了解每个人每天访问网站的情况）、FTP 记录（FTP 下载/上传记录，可以将 ftp 地址，用户名和密码全部记录下来，下载/上传的文件也进行保存。可以随时查看）、Telnet 记录（记录 Telnet 的使用记录，BBS 访问的内容可以全部记录下来备查）、P2P 记录（记录通过 BT/Emule 进行的网络下载流量，及时发现带宽的滥用问题，通过网络记录功能，常见的网络带宽使用情况都可以进行分析和记录）、用户权限管理、基于用户监控内容（可以为每个用户

设定监控内容，监控指定用户的指定信息。对于不需要监控的用户，可以设定不监控）、用户分组、管理员权限管理、系统资源管理、查看服务器资源使用（显示服务器软硬件信息以及当前使用状况，CPU、内存和硬盘等使用情况，以便急时调整设置）、用户分析、基于用户的网络服务记录（可以根据用户对各种网络服务进行查看，当需要重点查看某用户的网络使用记录时，该功能可以非常方便地将该用户的网络使用情况列出）、用户流量分析（以排名方式列出每个用户的网络流量使用情况，方便网络管理人员决定如何调整网络带宽分配）、报表生成（服务流量报表将每日各种网络服务的流量状况以图表形式显示出来，可以看出每个时间段网络的使用情况，为网络管理人员调整网络管理状况提供依据）、统计信息、离线日报表（生成 PDF 格式的日报表，直接发送到管理员信箱，无须连接到服务器也可以直接查看报表）、Top10（用户网络使用 Top10 针对每种网络应用，列出 Top10 用户图表，该图表可以选择开放给所有用户，以便让每个用户都可以看到自己的网络应用情况，从而由完全的被动管理转向主动，自觉的自我管理，用户在发现自己在 Top10 名列前茅之后，如果是非工作相关的流量，则会意识到自己有可能会被管理人员注意到，从而进行主动的自我约束，减少非工作网络使用。企业的工作效率可以因此而获得提升）、数据库管理、数据备份、数据恢复和数据清除。

6. Ratproxy

Ratproxy 是 Google 的一款内部安全工具，可以分析很多问题，如存在威胁的跨站脚本包含、对伪造的跨站请求防范不足、缓存问题，潜在的 XSS、可能不安全的跨站代码包含策略、信息泄露，不一而足。用于被动地审核 Web 应用的安全性。作为一款被动工具，Ratproxy 会监视浏览器与 Web 应用之间的交互。它的工作方式使它比传统方法具备以下优势：不会破坏现有 Web 应用，低投入、高产出，可以保留用户与 Web 应用交互的控制流，在脚本行为中的 WYSIWYG（所见即所得）数据，简化了过程整合。Ratproxy 明确地关注当代 Web 2.0 应用中优先级最高的问题，为它们提供简明的报告，给予用户充分的自由，以可重复的方式来完成这些工作。用户不会再被大量原始的 HTTP 流量数据淹没，而且这个工具远不仅仅是一个人工干预应用程序的框架。

7. S_Audit

S_Audit 网络安全审计系统能够在不影响网络自身性能的前提下，实现对网络进行全面的安全审计，全面掌握网络内部的使用情况。系统可以检测并记录网络内部传输的信息，及时发现并制止机密信息的泄露和窃取，减少网络资源的滥用，制止网络中的违规行为。系统强大的网络安全审计能力极大地增强了网络安全整体防范和预警能力，适用于政府、金融、电信和大型事业单位等各个领域中相对隔离的网络环境。主要功能为支持多种典型应用的全面审计，包括 Telnet、HTTP、FTP、SMTP 和 POP3 等；全面记录并能完整还原应用全过程、针对 NetBIOS/Samba 协议文件共享审计功能；对重要客户机重要文件和目录进行防护，实现主机服务端口审计功能；能够及时、有效地发现主机

系统是否被黑客设置后门，发现系统中异常的服务；具备强大的流量监测和历史流量查询功能，图形化显示网络应用情况，发现网络异常流量以及峰值瓶颈，提供灵活的用户自定义审计功能；实现用户对特定网络应用进行的审计需求，提供完善和丰富的，包括专业化报表和分析图形在内的报表功能，并支持 E-mail 自动发送功能，同时支持通过 Web 方式和客户端方式查看报警。具有如下特点：多种审计类型可供选择，有效地对全网进行安全审计；强大的审计还原能力，可对审计内容进行直观再现；可自定义审计规则，满足用户的非典型环境审计的需要；多样化的安全响应措施，支持记录、报警、中断、防火墙联动，报警到网管系统等手段；专业化的安全规则配置向导，灵活的规则设置功能；采用旁路式网络接入技术，不需更改任何网络拓扑，不影响网络应用；适应各种环境的网络接入，支持百兆、千兆和 2.5G POS 等网络环境；层次化、易扩展型的体系结构；完善的集中告警功能与强大的远程管理功能。

4.15　安全管理制度

4.15.1　信息安全管理制度的内容

信息安全管理制度是通过维护信息的机密、完整性和可用性，来识别、评估、管理和保护组织所有的信息资产，制定和实施安全策略、安全标准、安全方针和安全措施的一种体制。计算机及其网络系统的安全管理是计算机安全的重要组成部分，安全管理贯穿于计算机网络系统设计、运行和维护的各个阶段，既包括行政手段，又包括技术措施。在系统的设计阶段，应该制定出网络系统的安全策略；在工程设计阶段，应该按照安全策略的要求制定系统的安全机制；在系统的运行中，应该强制执行安全机制所要求的各项安全措施和安全管理原则，并且经过风险分析和安全审计来检查和评估，不断补充、改进和完善安全措施。

安全管理制度主要包括管理制度、制定和发布、评审和修订。不同等级的基本要求在安全管理制度方面所体现的不同在三个方面都有所体现。一级安全管理制度要求：主要明确了制定日常常用的管理制度，并对管理制度的制定和发布提出基本要求。二级安全管理制度要求：在控制点上增加了评审和修订，管理制度增加了总体方针和安全策略，以及对各类重要操作建立规程的要求，并且管理制度的制定和发布要求组织论证。三级安全管理制度要求：在二级要求的基础上，要求机构形成信息安全管理制度体系，对管理制度的制定要求和发布过程进一步严格和规范。对安全制度的评审和修订要求领导小组的负责。四级安全管理制度要求：在三级要求的基础上，主要考虑了对带有密级的管理制度的管理和管理制度的日常维护等。

表 4-11 表明了安全管理制度在控制点上逐级变化的特点。

表 4-11　安全管理制度控制点的逐级变化

控　制　点	一　　级	二　　级	三　　级	四　　级
管理制度	√	√	√	√
制定和发布	√	√	√	√
评审和修订		√	√	√
合计	2	3	3	3

管理制度：信息安全管理制度文件通过为机构的每个人提供基本的规则、指南、定义，从而在机构中建立一套信息安全管理制度体系，防止员工的不安全行为引入风险。信息安全管理制度体系分为三层结构：总体方针、具体管理制度和各类操作规程。信息安全方针应当阐明管理层的承诺，提出机构管理信息安全的方法；具体的信息安全管理制度是在信息安全方针的框架内，为保证安全管理活动中的各类管理内容的有效执行而制定的具体的信息安全实施规则，以规范安全管理活动，约束人员的行为方式；操作规程是为进行某项活动所规定的途径或方法，是有效实施信息安全政策、安全目标与要求的具体措施。这三层体系化结构完整地覆盖了机构进行信息安全管理所需的各类文件化指导。

制定和发布：制定安全管理制度是规范各种保护单位信息资源的安全活动的重要一步，制定人员应充分了解机构的业务特征（包括业务内容、性质、目标及其价值），只有这样才能发现并分析机构业务所处的实际运行环境，并在此基础上提出合理的、与机构业务目标相一致的安全保障措施，定义出与管理相结合的控制方法，从而制定有效的信息安全政策和制度。机构高级管理人员参与制定过程，有利于：

（1）制定的信息安全政策与单位的业务目标一致。

（2）制定的安全方针政策、制度可以在机构上下得到有效的贯彻。

（3）可以得到有效的资源保障，如在制定安全政策时必要的资金与人力资源的支持，及跨部门之间的协调问题都必须由高层管理人员来推动。

在制定安全管理制度中，各种文档的制定非常重要，主要包括如下文档。

- 网络建设方案文档：网络技术体制、网络拓扑结构、设备配置、IP 地址和域名分配方案等相关技术文档。
- 机房管理制度文档：包括对网络机房实行分域控制，保护重点网络设备和服务器的物理安全。
- 各类人员职责分工：根据职责分离和多人负责的原则，划分部门和人员职责，包括对领导、网络管理员、安全保密员和网络用户职责进行分工。
- 安全保密规定文档：制定颁布本部门计算机网络安全保密管理规定。
- 网络安全方案：网络安全项目规划、分步实施方案、安全监控中心建设方案和安全等级划分等整体安全策略。

- 安全策略文档：建立防火墙、入侵检测、安全扫描和防病毒系统等安全设备的安全配置和升级策略以及策略修改登记。
- 口令管理制度：严格网络设备、安全设备、应用系统以及个人计算机的口令管理制度。
- 系统操作规程：对不同应用系统明确操作规程，规范网络行为。
- 应急响应方案：建立网络数据备份策略和安全应急方案，确保网络的应急响应。
- 用户授权管理：以最小权限原则对网络用户划分数据库等应用系统操作权限，并做记录。
- 安全防护记录：记录重大网络安全事件，对网络设备和安全系统进行日志分析，并提出修复意见；定期对系统运行、用户操作等进行安全评估，提交网络安全报告。
- 评审和修订：安全政策和制度文件制定实施后，机构要定期评审安全政策和制度，并进行持续改进，尤其当发生重大安全事故、出现新的漏洞以及技术基础结构发生变更时。因为机构所处的内外环境是不断变化的，信息资产所面临的风险也是一个变数，机构中人的思想、观念也在不断变化。在这个不断变化的世界中，要想保证本系统的安全性，就要对控制措施和信息安全政策与制度持续改进，使之在理论上、标准上及方法上与时俱进。

其他制度文档还有信息发布审批、设备安装维护管理规定、人员培训和应用系统等，以及全面建立计算机网络各类文档，堵塞安全管理漏洞。

在安全管理中，最活跃的因素是人，对人的管理包括法律、法规与政策的约束、安全指南的帮助、安全意识的提高、安全技能的培训、人力资源管理措施以及企业文化的熏陶，这些功能的实现都是以完备的安全管理政策和制度为前提。信息安全有三条基本的管理原则：从不单独工作、限制使用期限和责任分散。从不单独工作原则指的是在人员条件许可的情况下，由最高领导人指派两个或者多个可靠而且能够胜任工作的专业人员，共同参与每项与安全相关的活动，并且通过签字、记录和注册等方式证明。限制使用期限原则指的是任何人都不能在一个与安全有关的岗位上工作太长时间，工作人员应该经常轮换工作，这种轮换依赖于全体人员的诚实度。责任分散原则指的是在工作人员素质和数量允许的情况下，不集中于一人实施全部与安全有关的功能，由不同的人和小组来执行。安全管理制度包括信息安全工作的总体方针、策略、规范各种安全管理活动的管理制度以及管理人员或操作人员日常操作的操作规程，安全风险管理、安全策略和安全教育构成了整个信息安全管理体系。

4.15.2 安全风险管理

信息系统的安全风险，是指由于系统存在的脆弱性，人为或自然的威胁导致安全事件发生所造成的影响。信息安全风险评估，则是指依据国家有关信息安全技术标准，对

信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行科学评价的过程，它要评估信息系统的脆弱性、信息系统面临的威胁以及脆弱性被威胁源利用后所产生的实际负面影响，并根据安全事件发生的可能性和负面影响的程度来识别信息系统的安全风险。信息安全风险评估是信息安全保障体系建立过程中重要的评价方法和决策机制。没有准确及时的风险评估，将使得各个机构无法对其信息安全的状况做出准确的判断。

风险评估的准备过程是组织进行风险评估的基础，是整个风险评估过程有效性的保证。组织对自身信息及信息系统进行风险评估的结果将受到业务需求及战略目标、文化、业务流程、安全要求、规模和结构的影响。不同组织对于风险评估的实施过程可能存在不同的要求，因此在风险评估实施前，应该考虑如下问题。

（1）确定风险评估的范围。进行风险评估可能是由于自身商业要求及战略目标的要求，相关方的要求或其他原因，因此应根据上述原因确定风险评估范围。范围可能是组织全部的信息和信息系统，可能是单独的信息系统，可能是组织的关键业务流程，也可能是客户的知识产权。

（2）确定风险评估的目标。组织应明确风险评估的目标，为风险评估的过程提供导向。支持组织的信息、系统、应用软件和网络是组织重要的资产。资产的保密性、完整性和可用性对于维持竞争优势、现金流动、获利能力、法规要求和组织形象是必要的。组织要面对来自四面八方日益增长的安全威胁，系统、应用软件和网络可能是严重威胁的目标。同时，由于组织的信息化程度不断提高，对基于信息系统和服务技术的依赖日益增加，一个组织则可能出现更多的脆弱性。组织的风险评估的目标基本上来源于组织业务持续发展的需要、满足相关方的要求、满足法律法规的要求等方面。

（3）建立适当的组织结构。在风险评估过程中，组织应建立适当的组织结构，以支持整个过程的推进，如成立由管理层、相关业务骨干和 IT 技术人员等组成的风险评估小组。组织结构的建立应考虑其结构和复杂程度，以保证能够满足风险评估的范围和目标。

（4）建立系统性的风险评估方法。风险评估方法应通过考虑评估的范围、目的、时间、效果、组织文化、人员素质以及开展程度等因素来确定，使之能够与环境和安全要求相适应。

（5）获得最高管理者对风险评估策划的批准。上述所有内容应得到组织的最高管理者的批准，并对管理层和员工进行传达。

根据评估实施者的不同，将风险评估形式分为自评估和他评估两大类。自评估是由被评估信息系统的拥有者依靠自身的力量，对其自身的信息系统进行的风险评估活动。他评估则是被评估信息系统拥有者的上级主管机关或业务主管机关发起的，依据已经颁布的法规或标准进行的具有强制意味的检查活动，是通过行政手段加强信息安全的重要措施。他评估也是经常提及的检查评估，自评估和他评估都可以通过信息安全风险评估服务机构进行风险评估的咨询、服务、培训以及风险评估有关工具的提供。

风险评估的基本要素为脆弱性、资产、威胁、风险和安全措施，与这些要素相关的属性分别为业务战略、资产价值、安全需求、安全事件和残余风险，也是风险评估要素的一部分。风险评估的工作是围绕其基本要素展开的，在对这些要素的评估过程中需要充分考虑业务战略、资产价值、安全事件和残余风险等与这些基本要素相关的各类因素。这些要素之间存在着以下关系：业务战略依赖于资产去完成；资产拥有价值，单位的业务战略越重要，对资产的依赖度越高，资产的价值则就越大，风险也越大，并可能演变成安全事件；威胁都要利用脆弱性，脆弱性越大则风险越大；脆弱性使资产暴露，是未被满足的安全需求，威胁要通过利用脆弱性来危害资产，从而形成风险；资产的重要性和对风险的意识会导出安全需求；安全需求要通过安全措施来得以满足，且是有成本的；安全措施可以抗击威胁，降低风险，减弱安全事件的影响；风险不可能也没有必要降为零，在实施了安全措施后还会有残留下来的风险——一部分残余风险来自于安全措施可能不当或无效，在以后需要继续控制这部分风险，另一部分残余风险则是在综合考虑了安全的成本与资产价值后，有意未去控制的风险，这部分风险是可以被接受的；残余风险应受到密切监视，因为它可能会在将来诱发新的安全事件，如图 4-135 所示。

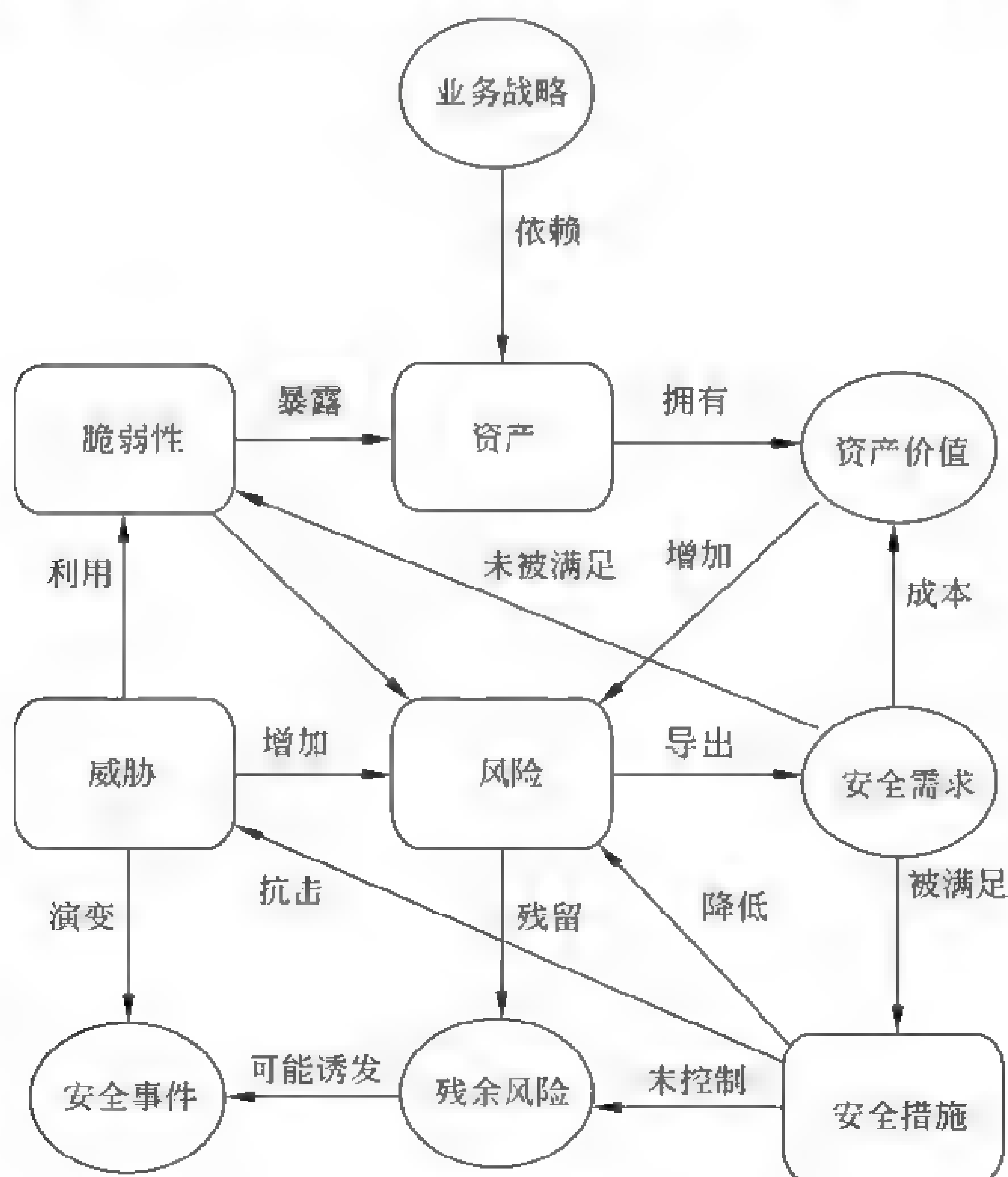


图 4-135　风险评估各要素关系图

在一般的评估体系中，资产大多属于不同的信息系统，业务生产系统的数量还可能会很多，需要将信息系统及其中的信息资产进行恰当的分类，才能进行下一步的风险评估工作。在实际项目中，具体的资产分类方法根据具体环境由评估者来灵活把握。资产赋值是对资产安全价值的估价，而不是以资产的账面价格来衡量。在对资产进行估价时，不仅要考虑资产的成本价格，还要考虑资产对于组织业务的安全重要性，即根据资产损失所引发的潜在商务影响来决定。为确保资产估价时的一致性和准确性，机构应该建立一个资产价值尺度，明确如何对资产进行赋值。资产估价的过程也就是对资产保密性、完整性和可用性影响分析的过程。影响就是由人为或突发性引起的安全事件对资产破坏的后果，这一后果可能毁灭某些资产，危及信息系统并使其丧失保密性、完整性和可用性，最终还会导致财政损失、市场份额或公司形象的损失。特别重要的是，即使每一次影响引起的损失并不大，但长期积累的众多意外事件的影响总和则可造成严重损失。一般情况下，影响主要从以下几方面来考虑。

（1）违反了有关法律或（和）规章制度。

（2）影响了业务执行。

（3）造成了信誉、声誉损失。

（4）侵犯了个人隐私。

（5）造成了人身伤害。

（6）对法律实施造成了负面影响。

（7）侵犯了商业机密。

（8）违反了社会公共准则。

（9）造成了经济损失。

（10）破坏了业务活动。

（11）危害了公共安全。

资产安全属性的不同通常也意味着安全控制、保护功能需求的不同。通过考察保密性、完整性和可用性三种不同安全属性，能够基本反映资产的价值。

安全威胁是一种对机构及其资产构成潜在破坏的可能性因素或者事件。无论对于多么安全的信息系统，安全威胁是一个客观存在的事物，它是风险评估的重要因素之一。产生安全威胁的主要因素可以分为人为因素和环境因素。人为因素又可区分为有意和无意两种。环境因素包括自然界不可抗的因素和其他物理因素。威胁作用形式可以是对信息系统直接或间接的攻击，例如非授权的泄露、篡改和删除等，在保密性、完整性或可用性等方面造成损害。也可能是偶发的或蓄意的事件。一般来说，威胁总是要利用网络、系统、应用或数据的弱点才可能成功地对资产造成伤害。安全事件及其后果是分析威胁的重要依据。但是，有相当一部分威胁发生时，由于未能造成后果，或者没有意识到，而被安全管理人员忽略。这将导致对安全威胁的认识出现偏差。在威胁评估过程中，首先就要对组织需要保护的每一项关键资产进行威胁识别。在威胁识别过程中，应根据资

产所处的环境条件和资产以前遭受威胁损害的情况来判断。一项资产可能面临着多个威胁，同样一个威胁可能对不同的资产造成影响。

脆弱性评估是安全风险评估中重要的内容。弱点包括物理环境、组织、过程、人员、管理、配置、硬件、软件和信息等各种资产的脆弱性。弱点是资产本身存在的，它可以被威胁利用、引起资产或商业目标的损害。值得注意的是，弱点虽然是资产本身固有的，但它本身不会造成损失，只是一种条件或环境，可能导致被威胁利用而造成资产损失。如果没有相应的威胁发生，单纯的弱点并不会对资产造成损害。那些没有安全威胁的弱点可以不需要实施安全保护措施，但它们必须记录下来以确保当环境、条件有所变化时能随之加以改变。需要注意的是，不正确的、起不到应有作用的或没有正确实施的安全保护措施本身就可能是一个安全薄弱环节。脆弱性评估将针对每一项需要保护的信息资产，找出每一种威胁所能利用的脆弱性，并对脆弱性的严重程度进行评估，即对脆弱性被威胁利用的可能性进行评估，最终为其赋相对等级值。在进行脆弱性评估时，提供的数据应该来自于这些资产的拥有者或使用者，来自于相关业务领域的专家以及软硬件信息系统方面的专业人员。脆弱性评估所采用的方法主要有问卷调查、人员问询、工具扫描、手动检查、文档审查和渗透测试等。脆弱性主要从技术和管理两个方面进行评估，涉及物理层、网络层、系统层、应用层和管理层等各个层面的安全问题。其中，在技术方面主要是通过远程和本地两种方式进行系统扫描、对网络设备和主机等进行人工抽查，以保证技术脆弱性评估的全面性和有效性；管理脆弱性评估方面可以按照 BS7799 等标准的安全管理要求对现有的安全管理制度及其执行情况进行检查，发现其中的管理漏洞和不足。

风险计算模型包含信息资产、弱点/脆弱性和威胁等关键要素。每个要素有各自的属性，信息资产的属性是资产价值，弱点的属性是弱点被威胁利用后对资产带来的影响的严重程度，威胁的属性是威胁发生的可能性。风险计算的过程如下。

（1）对信息资产进行识别，并对资产赋值。

（2）对威胁进行分析，并对威胁发生的可能性赋值。

（3）识别信息资产的脆弱性，并对弱点的严重程度赋值。

（4）根据威胁和脆弱性计算安全事件发生的可能性。

（5）结合信息资产的重要性和在此资产上发生安全事件的可能性计算信息资产的风险值。

4.15.3 信息安全策略

信息安全策略是信息安全管理的重要组成部分，在制定信息安全策略时必须遵循三个原则：严格的法律、法规是保障信息系统安全的坚强后盾；先进的网络安全技术与安全产品是信息安全的根本保证；先进严格的安全管理是确保信息安全策略实施的基础。随着网络应用以及网络安全技术的不断发展，安全策略的制订和实施是一个动态的延续

过程，可以请有经验的安全专家或购买服务商的专业服务。网络安全服务建设不可能仅依靠公司提供的安全服务，不是所有的网络都需要所有的安全技术，何况有些安全技术本身并不成熟，只有采取适当防护、重点突出的策略，才能有的放矢，不会盲目跟风。不同的网络有不同的安全需求，内部局域网和因特网接入有不同的要求，涉密计算机的管理与非涉密计算机的管理不同。应该遵照国家和本部门有关信息安全的技术标准和管理规范，针对本部门专项应用，对数据管理和系统流程的各个环节进行安全评估，确定使用的安全技术，设定安全应用等级，明确人员职责，制定安全分步实施方案，达到安全和应用的科学平衡。网络安全最大的威胁不是来自外部，而是内部人员对网络安全知识的缺乏。人是信息安全目标实现的主体，网络安全需要全体人员共同努力，避免出现“木桶效应”。信息安全策略应该全面地保护信息系统整体的安全，在设计时主要考虑如下几个方面的问题。

1．物理安全策略

物理安全是指在物理介质层次上对存储和传输的网络信息进行安全保护，是网络信息安全的基本保障。建立物理安全体系结构应从三个方面考虑：一是自然灾害、物理损坏和设备故障；二是电磁辐射、乘机而入、痕迹泄露等；三是操作失误、意外疏漏等。物理网络的基础设施包括物理介质的选择和网络拓扑结构。从安全的角度看，应根据电缆中所传输信息的敏感程度来为不同网段选择电缆的类型。网络传输中最常见的三种电缆包括双绞线、同轴电缆和光缆。光缆在高带宽和长距离传输的情况下用的最多。与双绞线或同轴电缆不同的是，光缆不辐射能量，能够有效地阻止窃听，而且比双绞线同轴电缆更难搭线窃听。物理安全控制是对物理基础设施、物理设备安全和物理访问的控制。对于现有的网络，如果为了适应已经改变的环境而正在创建或修改安全策略，就有必要更改物理基础设施，改变某些关键设备的物理位置，使安全策略更容易实施。如果已经将物理安全控制与安全策略相结合，那么当企业需要扩充和增加新的站点时，就应该在创建站点的同时考虑网络的物理安全控制。受限区域的物理访问需要主要根据分析或物理安全调查的结果来决定，严格限制接近机柜和关键网络基础设施设备所在地，除非经过授权或因工作需要，否则将禁止接近这些区域。设备问题可能会造成严重危害，当采用机柜放置所有关键的网络基础设施设备时，必须尽量使机柜处于一个独立的区域。当打印机密的配置文件或发送含配置内容的传真时，为了避免打印机或传真机的打印输出落入他人手中，需要将敏感打印机和传真机安装在 LAN 网段上，且该局域网应位于访问受到严格控制的室内。除此之外，还必须采取安全的方法来销毁打印输出和文档，如使用碎纸机。为保护关键的网络资源，必须安装和实施充分的环境安全保护。环境安全保护包括水灾的预防、监测和恢复；水害预防、监测和恢复；电源保护；温度控制；湿度控制；保护免受自然灾害的侵袭，包括地震、闪电和风暴等；保护不受过量磁场干扰；制定良好的清洁制度，减少尘土和垃圾。

机房和办公场地（放置终端计算机设备）的环境条件应该能够满足信息系统业务需

求和安全管理需求，具有基本的防震、防风和防雨等能力，机房场地应该符合选址要求，避免在建筑物的高层或地下室，以及用水设备的下层或隔壁，避免设在强电场、强磁场、强震动源、强噪声源、重度环境污染、易发生火灾、水灾、易遭受雷击的地区，不存在因机房和办公场地环境条件引发的安全事件或安全隐患。如果某些环境条件不能满足，应该及时采取补救措施。机房和办公场地的设计/验收文档应该有机房和办公场地所在建筑能够具有防震、防风和防雨等能力的说明和机房场地的选址说明，与机房和办公场地实际情况相符合。为了业务或安全管理需要，可以对机房划分区域，在机房重要区域前设置交付或安装等过渡区域，对不同区域设置不同机房或者同一机房的不同区域之间设置有效的物理隔离装置（如隔墙等），对各个区域都有专门的管理要求。机房不存在电子门禁系统控制之外的出入口，在访问机房和办公场地时，机房安全管理制度应该有关于机房出入方面的规定，机房出入口有专人值守，机房值守人员认真执行有关机房出入的管理制度，对进入机房的人员记录在案，进入机房要有审批记录和身份鉴别措施（如戴有可见的身份辨识标识）。有验收文档或产品安全资质的电子门禁系统运行、维护记录要定期检查，确定能够鉴别和记录进入的人员身份。

设备和介质等应该有防止丢失的保护措施，主要设备放置位置做到安全可控，设备或主要部件进行固定和标记，通信线缆铺设在隐蔽处，设置冗余或并行的通信线路，对机房安装的防盗报警系统和监控报警系统进行定期维护检查。在介质管理中，介质应该存放在介质库或档案室中，并且进行分类标识，设备或存储介质携带出工作环境要有审批程序、内容加密和专人检查等安全保护的措施。机房防盗报警设施、摄像、传感等监控报警系统以及运行、记录和报警记录确保正常运行。有关设备或存储介质携带出工作环境要有审批记录，以及专人对内容加密进行检查的记录；设备管理制度文档、通信线路布线文档、介质管理制度文档、介质清单和使用记录、机房防盗报警设施的安全资质材料、安装测试/验收报告等文档中的条文应该与设备放置位置、设备或主要部件保护、通信线缆铺设等实际情况一致。

为防止雷击事件导致重要设备被破坏需要采取一些防护措施，机房建筑设置通过验收或国家有关部门的技术检测的避雷装置，机房计算机系统接地设置专用地线，在电源和信号线增加有资质的避雷装置，以避免感应雷击。机房建筑避雷装置有人定期进行检查和维护，机房计算机系统接地（交流工作接地、安全保护接地）符合 GB50174－93《电子计算机机房设计规范》的要求。机房建筑防雷设计/验收文档、机房接地设计/验收文档、地线连接要求的描述与实际情况一致。机房要设置灭火设备和自动检测火情、自动报警、自动灭火的自动消防系统，有专人负责维护该系统的运行，制订有关机房消防的管理制度和消防预案，且定期进行消防培训，机房出现的消防安全隐患能够及时报告并得到排除。自动消防系统的摆放位置合理，有效期合格，运行记录、报警记录、定期检查和维修记录一切正常。机房消防方面的管理制度文档、机房防火设计/验收文档、自动消防系统的设计/验收文档、建筑材料、区域隔离防火措施的验收文档或消防、检查验收

文档与现有消防配置状况一致。机房可以采取区域隔离防火措施，将重要设备与其他设备隔离开。机房建设应该有防水防潮措施，如果机房内有上下水管安装，避免穿过屋顶和活动地板，穿过墙壁和楼板的水管要采取保护措施，如设置套管等方法。在湿度较高地区有人负责机房防水防潮事宜，配备除湿装置，防水防潮处理记录和除湿装置运行记录，与机房湿度记录情况一致。机房要定期检查是否出现漏水和返潮事件，如果出现机房水蒸气结露和地下积水的转移与渗透现象需要采取防范措施。机房的建筑防水和防潮设计/验收文档与机房防水防潮的实际情况一致。机房应该采用必要的接地等防静电措施和控制机房湿度的措施，控制在 GB2887 中规定的范围内，在静电较强地区的机房采取有效的防静电措施（如防静电地板、防静电工作台以及静电消除剂和静电消除器等）。机房防静电设计/验收文档中描述的内容与实际情况一致。机房应该配备恒温恒湿系统，保证温湿度能够满足计算机设备运行的要求，定期检查和维护机房的温湿度自动调节设施，在机房管理制度中规定温湿度控制的要求，有专门的人负责此项工作。温湿度记录、运行记录和维护记录、机房温、湿度满足 GB/2887-89《计算站场地技术条件》的要求。

计算机系统供电线路与其他供电分开且设置稳压器和过电压防护设备及短期备用电源设备（如 UPS），供电时间满足系统最低电力供应需求，安装冗余或并行的电力电缆线路（如双路供电方式），建立备用供电系统（如备用发电机）。计算机系统供电线路上的稳压器、过电压防护设备和短期备用电源设备等需要进行定期检查和维护，能够控制电源稳压范围满足计算机系统运行正常，计算机系统供电与其他供电分开。机房的电力供应安全设计/验收文档中标明单独为计算机系统供电，配备稳压器、过电压防护设备、备用电源设备以及冗余或并行的电力电缆线路等要求与机房电力供应实际情况是否一致。有防止外界电磁干扰和设备寄生耦合干扰的措施（包括设备外壳有良好的接地，电源线和通信线缆隔离等），并且对处理秘密级信息的设备采取防止电磁泄露的措施。对设备外壳进行良好的接地，电源线和通信线缆隔离，处理秘密级信息的设备为低辐射设备，安装满足 BMB4-2000《电磁干扰器技术要求和测试方法》要求的二级电磁干扰器。

2. 网络安全策略

为保护网络的安全，必须对访问系统及其数据的人进行识别，并检查其合法身份，对进入网络系统进行控制。访问控制首先要把用户和数据进行分类，然后根据需要把二者匹配起来，把数据的不同访问权限授予用户，只有被授权的用户才能访问相应的数据。在大型网络中，从源节点到目的节点可能有多条线路，有些线路可能是安全的，有些是不安全的。通过选择路由控制机制，可使信息发送者选择特殊路由，以保证数据的安全。网络安全中的访问控制分为两类：入系统访问控制和选择性访问控制。入系统访问控制为系统提供了第一层访问控制，控制着可以登录到服务器网络操作系统并获取系统资源的用户，通过用户名识别和验证、用户口令识别和验证以及用户账号的默认限制检查进入系统。选择性访问控制是基于主体或主体所在组的身份，这种访问控制是可选择性的，

如果一个主体具有某种访问权，则它可以直接或间接地把这种控制权传递给别的主体。选择性访问控制被内置于许多操作系统当中，是任何安全措施的重要组成部分。文件拥有者可以授予一个用户或一组用户访问权。网络上的选择性访问控制应对用户的访问权限进行控制：某人可以访问什么程序和服务？某人可以访问什么文件？谁可以创建、读或删除某个特定的文件？谁是管理员或“超级用户”？谁可以创建、删除和管理用户？某人属于什么组以及相关的权利是什么？当使用某个文件或目录时，用户有哪些权利？访问控制还包括对网络服务、数据库和其他应用系统的控制。

3. 系统安全策略

系统安全策略可以分为两大类来考虑，即强制安全策略和自主安全策略。系统的策略实施机制也划分为两部分：强制安全策略实施机制和自主安全策略实施机制，强制安全策略具有更好的普遍适用性，由系统强制提供，可涉及保密性、完整性、可用性和责任可查性等。自主安全策略将反映用户自主的安全需求，由于用户自主安全需求的多样性，为尽可能实施灵活的自主安全策略，系统应为用户提供方便的自主安全策略表达机制，如安全规则的说明工具。用户说明的与自主安全策略对应的规则集有时非常复杂，需要有专门的策略检查机制来确保规则的完备性、正确性和一致性。这些自主说明的安全规则只有通过检查处理后，才能形成适合于自主安全策略实施机制使用的系统内部自主安全策略（或规则集）。规则的内涵及内部表示方式的不同，又对自主安全策略实施机制提出了不同的要求，自主策略实施机制应能够为不同类型的规则提供执行能力。系统安全从低到高分为4级：D级是最低的安全级别，拥有这个级别的操作系统就像一个门户大开的房子，任何人可以自由进出，是完全不可信的。C级有两个安全子级别：C1和C2。C1级被称为选择性安全保护系统，描述了一种典型的用在UNIX系统上的安全级别。这种级别的系统对硬件有某种程度的保护，用户拥有注册账号和口令，系统通过账号和口令来识别用户是否合法，并决定用户对程序和信息拥有什么样的访问权，但硬件受到损害的可能性仍然存在。除了C1级包含的特性外，C2级别应具有访问控制环境权力。该环境具有进一步限制用户执行某些命令或访问某些文件的权限，而且还加入了身份认证级别。B级中有三个级别，B1级是支持多级安全（例如秘密和绝密）的第一个级别，这个级别说明处于强制性访问控制之下的对象，系统不允许文件的拥有者改变其许可权限。B2级要求计算机系统中所有的对象都要加上标签，而且给设备（磁盘、磁带和终端）分配单个或多个安全级别。它是提供较高安全级别的对象与较低安全级别的对象相互通信的第一个级别。B3级使用安装硬件的方式来加强域的安全，例如，内存管理硬件用于保护安全域免遭无授权访问或其他安全域对象的修改。A级是当前橙皮书的最高级别，它包括了一个严格的设计、控制和验证过程，该级别包含了较低级别的所有特性。黑客对系统的攻击和计算机病毒是系统安全的两大威胁，对于网络操作系统的安全管理，系统安装完后，应该给予指定的系统管理员与Supervisor/Admin等同的管理权限。获取对操作系统访问权的用户，给予注册、登记，授予对系统访问的账户和口令。定期做好

操作系统和应用程序的备份，对系统在运行过程中发生的错误作出详细的记录和归档，认真细致地分析每天的日志，对系统进行事后审计、监督和跟踪，建立操作系统所有资料的使用管理机制，及时做好系统版本的升级、打补丁、防病毒和系统的加固。

4．数据加密策略

访问控制只是控制可以获准进入计算机信息系统的对象，在计算机的应用中产生了大量需要存储和传输的数据，此时，有意的计算机犯罪和无意的数据破坏成为了最大的威胁。数据保密就是保护网络中各系统之间的交换数据，防止因数据被截获而造成泄密。数据保密主要包括连接保密（对某个连接上的所有用户数据提供保密）、选择字段保密（对协议数据单元的一部分选择字段进行保密）和信息流保密（对可能从观察信息流就能推导出的信息提供保密）。数据完整性保证接收方收到的信息与发送方发送的信息完全一致，它包括可恢复的完整性、无恢复的完整性和选择字段的完整性，主要通过数字签名技术来实现。对称密码和公钥密码是当前计算机信息系统中的两类基本加密算法。信息加密策略的制定应该根据网络系统的实际情况和需求来定，没有一个固定的模式，一般包括信息的分类和存储、信息的传输、备份介质存储。对于敏感信息，策略应该描述加密压缩的软件、转交的服务器名称、存储目录体系和归档时间。PKI 是一种具有普遍适用性的网络安全基础设备，是一套硬件、软件系统和安全策略的集合，它提供了一种安全机制，使用户在不知道对方身份和分布地的情况下，以数字证书为基础，通过一系列的信任关系来实现信息的真实性、完整性、保密性和不可否认性。PKI 定义了密码系统使用的处理方法和原则，建立了一个组织信息安全方面的指导方针，包含在实践中增强和支持安全策略的一些操作过程的详细文档、处理密钥和有价值信息的方法及根据风险级别定义安全控制级别。

5．信息安全组织管理策略

信息安全组织管理的目标和任务是利用管理学的原理构建信息安全团队，对信息安全事件作出及时、快速、准确的响应，确定并及时排除突发事件，使其服务对象的风险和损失降低到最低。无论是何种信息安全团队，其组织架构基本上是一样的，主要由决策层、管理层、执行层和信息管理系统 4 个部分组成。决策层负责制定信息安全团队的工作方针、政策以及相关的规章制度，对团队的建立负有决定性的作用，必须对安全事件的响应作出正确的判断。管理层主要负责团队的日常工作、内外部信息资产、财物和工作人员的管理。执行层负责对系统运行进行日常的维护和管理，对安全事故进行响应支持，对相关人员进行安全技术培训。信息管理系统负责决策层和管理层之间、管理层与执行层之间、执行层与用户层、决策层与执行层之间信息的处理和传递。关于人员录用，应指定或授权专门的部门或人员负责，严格规范人员录用过程，对被录用人员的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核，签署保密协议，从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。关于人员离岗，应制定有关管理规范，严格规范人员离岗过程，及时终止离岗员工的所有访问权限，取回

各种身份证件、钥匙、徽章等以及机构提供的软硬件设备，办理严格的调离手续，并承诺调离后的保密义务后方可离开。关于人员考核，应定期对各个岗位的人员进行安全技能及安全认知的考核，应对关键岗位的人员进行全面、严格的安全审查和技能考核，应建立保密制度，并定期或不定期地对保密制度执行情况进行检查或考核，应对考核结果进行记录并保存。

4.15.4 信息安全教育

计算机安全教育是计算机信息安全的重要组成部分，是增强人们安全意识和安全素质的有效方法。网络安全是一门新兴的技术，即便是对计算机专业人员来说也是一个崭新的领域，如果技术人员对安全产品只有一知半解，就不能对产品正确配置，甚至根本配置错误，不但大的安全投入得不到保护，而且带来虚假的安全。对于安全产品不能买回来一装了事，应该了解安全工具的局限性和双刃性以及错误的配置带来的问题。这要求技术人员不但要懂网络、懂安全，还要了解应用需求，了解网络协议、网络攻击手段，认清并处理网络病毒、密码攻击、分组窃听、IP 欺骗、拒绝服务、信任关系利用、端口攻击和未授权访问等多样化的攻击手段。 针对技术人员的培训包括网络安全理论培训、安全意识教育、岗位技能培训、安全技术培训、安全产品培训以及本部业务培训，对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训。对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒。应对安全教育和培训的情况及结果进行记录并归档保存。人始终是影响计算机信息系统安全的最大因素，对人的计算机信息系统法律法规的宣传教育、安全管理知识的学习和职业道德的教育是计算机信息系统安全教育的重点，通过制定、实施信息安全管理教育，对相关的人员进行安全培训，使他们真正掌握安全管理各方面的知识，才能使整套的安全策略和安全措施得到充分的执行和实施。

第 5 章　标准化和知识产权

标准化在经济发展中起着不可替代的重要作用。仅就一个网络规划设计项目来说，有多个层次、不同分工的人员相互配合，在项目的各个部分以及各个阶段之间也都存在着许多联系和衔接问题。如何把这些错综复杂的关系协调好，需要有一系列统一的约束和规定。这些约束和规定不断完善并被业界所普遍认可，这就是标准化。标准提供统一的行动规范和衡量准则，使得各种工作都能有章可循。无论是从技术层面还是从管理层面来看，标准化在整个 IT 业乃至社会发展中起着举足轻重的作用。作为一名网络规划设计师，标准化方面的知识是不可或缺的。

知识产权是现代社会发展中不可缺少的一种法律制度。知识产权的智力成果是一种无形财产权，是不同于普通产品的知识产品（智力成果）。只有实施软件产权保护，对软件产品的著作权进行保护，才会有利于软件产业的发展。为维护软件企业自身合法权益，创造者防止自己的智力创作受到侵害或者被复制，并像其他劳动者一样享受通过自己的努力而得到的成果，有必要建立和加强保护软件知识产权的法制意识，了解知识产权的归属关系。目前，涉及计算机技术和软件技术的知识产权法律有多种类型，如《中华人民共和国著作权法》（包括《计算机软件保护条例》）、《中华人民共和国专利法》、《中华人民共和国商标法》、《中华人民共和国反不正当竞争法》和《中华人民共和国合同法》等。它们根据不同的对象、内容和要求对保护的客体分别做出了规定。它们之间的关系并不是相互排斥的，而是可选的、并行的、交叉的和重叠的。遵守现行的法律是对人们的基本要求，这是必须的道德修养和守法行为。

通过本章的学习，要求掌握如下内容。

（1）了解标准及标准化的意义，熟悉标准化的过程。

（2）了解标准的种类与标准体系，熟悉标准的分类与编号。

（3）了解国际标准与国外先进标准及其标准化组织，熟悉采用国际标准及国外先进标准的程度。

（4）了解信息技术标准化，熟悉基本的信息管理标准化和网络工程标准化。

（5）了解质量管理体系标准 ISO 9000、软件能力成熟度模型（CMM）。

（6）了解软件知识产权的基本概念和特点，建立知识产权意识。

（7）了解计算机著作权侵权行为与法律保护，熟悉计算机著作权的权利及归属。

（8）了解反不正当竞争法，熟悉计算机网络的商业秘密。

5.1 标准化

5.1.1 标准化的基本概念

1．标准、标准化的定义

标准是对重复性事物和概念所做的统一规定。它以科学、技术和实践经验的综合成果为基础，经有关方面协商一致，由一个公认机构批准，以特定形式发布，作为共同遵守的准则和依据。

标准化是指在经济、技术、科学和管理等社会实践中，对重复性事物和概念通过制定、发布和实施标准达到统一，以获得最佳秩序和社会效益的活动。

2．标准化的范围和对象

在经济、技术、科学和管理等社会实践中，同一事物和概念反复或重复出现或进行，如同一产品的反复生产，同一方法的反复多次进行，同一技术的多次使用，同一概念的多次使用，同一管理事项的重复进行等，这些都可作为标准化的领域和对象。

3．标准化的本质和目的

统一是标准的本质特征，任何标准都是在一定条件下的“统一规定”。标准化的目的是获得最佳秩序和社会效益。

4．标准化的主要作用

标准化为科学管理奠定了基础，即依据生产技术的发展规律和客观经济规律对企业进行管理，而各种科学管理制度的形式都以标准化为基础。

标准化可以促进经济全面发展，提高经济效益。标准化应用于科学研究，可以避免在研究上的重复劳动；应用于产品设计，可以缩短设计周期；应用于生产，可使生产在科学的和有秩序的基础上进行；应用于管理，可促进统一、协调和高效率等。

标准化是科研、生产、使用三者之间的桥梁。一项新技术或科研成果，一旦纳入相应标准，就能迅速得到推广和应用，从而促进技术进步。

标准化为组织现代化生产创造了前提条件，通过制定和使用标准来保证各生产部门的活动在技术上保持高度的统一和协调，以使生产正常进行。

标准化可以促进对自然资源的合理利用，保持生态平衡，维护人类社会当前和长远的利益；合理发展产品品种，提高企业应变能力，以更好地满足社会需求；保证产品质量，维护消费者利益；在社会生产组成部分之间进行协调，确立共同遵循的准则，建立稳定的秩序；促进国际技术交流和贸易发展，提高产品在国际市场上的竞争能力；保障身体健康和生命安全。环保标准、卫生标准和安全标准制定、发布后，用法律形式强制执行，对保障人民的身体健康和生命财产安全具有重大作用。

5.1.2　标准化的基本过程

标准是标准化活动的产物，其目的和作用都是要通过制定和贯彻具体的标准来体现的。标准化是一个可分为几个子过程的活动过程，一般包括标准产生（调查、研究、形成草案、批准发布）子过程、标准实施（宣传、普及、监督、咨询）子过程和标准更新（复审、废止或修订）子过程等。

5.1.3　标准的分类

标准化工作是一项复杂的系统工程，标准为适应不同的要求从而构成一个庞大而复杂的系统。为便于研究和应用的目的，可以从不同的角度和属性将标准进行分类。

1．根据适用范围分类

（1）国际标准：由国际标准化团体制定、公布和通过的标准。通常，国际标准是指 ISO 和 IEC 以及 ISO 所出版的《国际标准题目关键词索引（KWIC Index）》中收录的其他国际组织制定、发布的标准等。国际标准在世界范围内统一使用，没有强制的含义，各国可以自愿采用。

（2）国家标准：由一个国家的政府或国家级的机构制定或批准，适用于全国范围的标准，如中国国家标准（GB）、美国国家标准（ANSI）、德国国家标准（DIN）、英国国家标准（BS）和日本国工业标准（JIS）等。

（3）区域标准：区域标准又称地区标准，泛指世界上按地理、经济或政治划分的某一区域标准化团体所通过的标准。

（4）行业标准：由行业机构、学术团体或国防机构制定，并适用于某个业务领域的标准，如美国电气和电子工程师学会标准（IEEE）、中华人民共和国国家军用标准（GJB）、美国军用标准（MIL-S）和美国国防部标准（DOD-STD）等。

（5）地方标准：由一个国家的地方一级行政机构（省、州或加盟共和国）制定的标准，称为地方标准。它一般由地方所属的各企业与单位执行。

（6）企业标准：由企业或公司批准、发布的标准，某些产品标准由其上级主管机构批准、发布。例如，美国 IBM 公司通用产品部制定的“程序设计开发指南”，仅供该公司内部使用。企业为达到或超过上级标准，而对产品质量指标制定高于现行上级标准的用于内部控制的企业标准，目的在于促进产品质量的提高。

（7）项目规范：由某一科研生产项目组织制定，且为该项任务专用的软件工程规范，如计算机集成制造系统（CIMS）的软件工程规范。

我国标准分为国家标准、行业标准、地方标准和企业标准 4 类。

2．根据性质分类

根据标准的性质有所不同，可分为技术标准、管理标准和工作标准。

3．根据对象和作用分类

根据标准的对象和作用，可分为基础标准、产品标准、方法标准、安全标准、卫生标准、环境保护标准和服务标准等。

4．根据法律约束性分类

根据标准的法律约束性，可分为强制性标准和推荐性标准。

5.1.4 标准的编号

1．国际、国外标准代号及编号

国际及国外标准代号形式各异，但基本结构为：

标准代号+专业类号+顺序号+年代号

其中，标准代号大多采用缩写字母，如 IEC 代表国际电工委员会（International Electrotechnical Commission）、API 代表美国石油协会（American Petroleum Institute）、ASTM 代表美国材料与试验协会（American Society for Testing and Materials）等；专业类号因其所采用的分类方法不同而各异，有字母、数字、字母数字混合式三种形式；标准号中的顺序号及年代号的形式与我国基本相同。例如，国际标准 ISO 代号及编号格式为"ISO+标准号 ＋[-＋ 分标准号]＋ ：+发布年号（方括号中的内容可有可无）"，如 ISO 8402：1987 和 ISO9000-1：1994 分别是 ISO 标准的编号。

2．我国标准代号及编号

我国标准的编号由标准代号、标准发布顺序号和标准发布年号构成。

（1）国家标准的代号由大写汉语拼音字母构成，强制性国家标准的代号为 GB，推荐性国家标准的代号为 GB/T。

（2）行业标准代号由大写汉语拼音字母组成，再加上斜线/和 T 组成推荐性行业标准（如××/T）。行业标准代号由国务院各有关行政主管部门提出其所管理的行业标准范围的申请报告，国务院标准化行政主管部门审查确定并正式公布该行业标准代号。已正式公布的行业代号有 QJ（航天）、SJ（电子）、JB（机械）和 JR（金融系统）等。

（3）地方标准代号由大写汉语拼音字母 DB 加上省、自治区、直辖市行政区域代码的前两位数字（如北京市为 11、天津市为 12、上海市为 31 等），再加上斜线/和 T 组成推荐性地方标准（DB××/T），不加斜线/和 T 的为强制性地方标准，如 DB××。

（4）企业标准的代号由大写汉语拼音字母 Q 加斜线再加企业代号组成（Q/×××），企业代号可用大写拼音字母或阿拉伯数字或两者兼用所组成。

5.1.5 国际标准及国外先进标准

1．国际标准

国际标准是指国际标准化组织、国际电工委员会（IEC）制定的标准，以及 ISO 为促进《关贸总协定——贸易技术壁垒协议》即标准守则的贯彻实施所出版的《国际标准

题目关键词索引（KWIC Index）》中收录的其他国际组织制定的标准。1989 年，KWIC 索引（第 2 版）收录了 ISO 与 IEC 以及其他 27 个国际组织的标准。

2．国外先进标准

国外先进标准是指未经国际标准化组织确认并公布的其他国际组织的标准，如国际上有权威的区域性标准、世界上主要经济发达国家的国家标准和通行的团体标准，包括知名跨国企业标准在内的其他国际上公认的先进标准。

（1）国际上有权威的区域性标准，如欧洲标准化委员会（CEN）、欧洲电工标准化委员会（CENELEC）、欧洲广播联盟（EBU）、亚洲大洋洲开放系统互联研讨会（AOW）和亚洲电子数据交换理事会（ASEB）等制定的标准。

（2）世界经济技术发达国家的国家标准，如美国国家标准、德国国家标准、英国国家标准、日本国工业标准、瑞典国家标准、法国国家标准（NF）、瑞士国家标准（SNV）、意大利国家标准（UNI）和俄罗斯国家标准（TOCTP）等。

（3）国际公认的行业性团体标准，如美国材料与实验协会标准（ASTM）、美国石油学会标准、美国军用标准（MIL）、美国保险商验所安全标准（UL）、美国电气制造商协会标准（NEMA）、美国电影电视工程师协会标准（SMPTE）、美国机械工程师协会标准（ASME）和英国劳氏船级社船舶人级规范（LR）等。

（4）国际公认的先进企业标准，如美国 IBM 公司、美国 HP 公司、芬兰诺基亚公司和瑞士钟表公司等企业标准。

5.1.6　采用国际标准和国外先进标准

采用国际标准和国外先进标准是指把国际标准和国外先进标准的内容，通过分析研究，不同程度地纳入我国的国家标准、行业标准、地方标准和企业标准，并且按照规定的程序进行起草、审批、发布、贯彻执行。采用国际标准或国外先进标准的程度分为等同采用、等效采用和非等效采用。

（1）等同采用国际标准是指在制定国家、专业或企业等标准时，把国际标准采纳到所制定的标准中，使得标准在技术上、编写上与国家标准相同，或编写上有编辑性修改。

（2）等效采用是指制定的标准与相应的国际标准在技术上只有小的差异，在编写方法上可以不完全相同。小的技术差异是指非实质性的差异，即这种差异可以被国际上认可并接受，如增加些事例或解释说明资料等。

（3）非等效采用是指制定的标准与国际标准在技术内容上有重大差异（制定的标准中有国际标准不能接受的条款，或者在国际标准中有所制定的标准不能接受的条款），但性能和质量水平与国际标准相当，在通用、互换、安全和卫生等方面与国际标准协调一致。在技术上有重大差异的情况下，虽然标准制定时是以国际标准为基础的，并在很大程度上与国际标准相适应，但不能使用“等效”这个术语。

采用程度符号用缩写字母表示，等同采用 idt 或 IDT 表示，等效采用 eqv 或 EQV，

非等效采用 neq 或 NEQ 表示。

5.1.7 标准化组织

1. 国际标准化组织

ISO 和 IEC 是世界上两个最大、最具有权威性的国际标准化组织。目前，由 ISO 确认并公布的国际标准化组织还有国际计量局（BIPM）、联合国教科文组织（UNESCO）、世界卫生组织（WHO）、世界知识产权组织（WIPO）、国际信息与文献联合会（FID）、国际法制计量组织（OIML）等。

2. 区域标准化组织

区域标准化组织是指同处一个地区的某些国家组成的标准化组织。区域是指世界上按地理、经济或民族利益划分的区域。参加组织的机构有的是政府性的，有的是非政府性的，是为发展同一地区或毗邻国家间的经济及贸易，维护该地区国家的利益，协调本地区各国标准和技术规范而建立的标准化机构，如欧洲标准化委员会、欧洲电工标准化委员会和亚洲标准咨询委员会（ASAC）等。其主要职能是制定、发布和协调该地区的标准。

3. 行业标准化组织

行业标准化组织是指制定和公布适应于某个业务领域标准的专业标准化团体，以及在其业务领域开展标准化工作的行业机构、学术团体或国防机构，如美国电气电子工程师学会、美国国防部（DOD）以及我国国防科学技术工业委员会（GJB）等。

4. 国家标准化组织

国家标准化组织是指在国家范围内建立的标准化机构以及政府确认（或承认）的标准化团体，或者接受政府标准化管理机构指导并具有权威性的民间标准化团体，如美国国家标准学会（ANSI）、英国标准学会（BSI）、德国标准化学会（DIN）、法国标准化协会（AFNOR）和日本工业标准调查会（JIS）等。

5.1.8 信息技术标准化

信息技术标准化是围绕信息技术的开发、信息产品的研制和信息系统建设、运行与管理而开展的一系列标准化工作。其中主要包括信息技术术语、信息表示、汉字信息处理技术、媒体、软件工程、数据库、网络通信、电子数据交换、电子卡、管理信息系统和计算机辅助技术等方面的标准化。

1. 信息编码标准化

编码是一种信息表现形式。在一定条件下，它对事物或概念的描述比自然语言要直接、简洁、准确和有力。要保证信息编码的一致性，就要对编码对象的确定、对象特性的选择、编码方法和代码设计进行标准化。对信息进行编码实际上是对文字、音频、图形和图像等信息进行处理，使之量化，从而便于利用各种通信设备进行信息传递和利用

计算机进行信息处理。为了统一编码系统，人们制定了各种标准代码，如国际上较通用的 ASCII 码等。

2．条码标准化

条码是一种特殊的代码，即一组规则排列的条、空及其对应字符组成的标记，用以表示一定的信息。条码中的条、空分别由两种不同深浅的颜色（通常为黑、白色）表示，并满足一定的光学对比度要求，其目的是便于光电扫描设备识读后将数据输入计算机。条码中的字符供人们直接识读，或通过键盘向计算机输入数据。目前国际上广泛使用的条码是国际物品编码协会的标准化条码 EAN。我国国家标准《GB 904-91 通用商品条码》中的通用商品条码的结构与 EAN 条码结构相同，由 13 位数字码以及对应的条码组成，即由前缀码（3 位）、制造厂商代码（4 位）、商品代码（5 位）和检验码（1 位）组成，3 位前缀码是标识国家或地区的代码，我国的国家代码为 690。

3．汉字编码标准化

汉字编码是将每一个汉字按一定的规律用若干个字母、数字、符号表示出来。汉字编码的方法很多，主要有数字编码、拼音编码和字形编码。我国在汉字编码标准化方面取得的突出成就就是信息交换用汉字编码字符集国家标准的制定。该字符集共有 6 个。其中，GB 2312-80 信息交换用汉字编码字符集是基本集，收入常用基本汉字和字符 7445 个；GB 7589-87 和 GB 7590～87 分别是第二辅助集和第四辅助集，各收入现代规范汉字 7426 个；GB/T 12345-90 是辅助集，它与第三辅助集和第五辅助集分别是与基本集、第二辅助集和第四辅助集相对应的繁体字的汉字字符集。除汉字编码标准化外，汉字信息处理标准化的内容还包括汉字键盘输入的标准化；汉字文字识别输入和语音识别输入的标准化；汉字输出字体和质量的标准化；汉字属性和汉语词语的标准化等。

4．软件工程标准化

随着软件工程学科的发展，人们对计算机软件的认识逐渐深入。软件工作的范围从只是使用程序设计语言编写程序扩展到整个软件生存期。软件工程的目的是改善软件开发的组织，降低开发成本，缩短开发时间，提高工作效率，提高软件质量。它在内容上包括软件开发的软件概念形成、需求分析、计划组织、系统分析与设计、结构程序设计、软件调试、软件测试和验收、软件安装和检验、软件运行和维护以及软件运行的终止。同时还有许多技术管理工作，如过程管理、产品管理、资源管理以及确认与验证工作，如评审与审计、产品分析等。软件工程最显著的特点就是把个别的、自发的、分散的、手工的软件开发变成一种社会化的软件生产方式。软件生产的社会化必然要求软件工程实行标准化。软件工程标准的类型也是多方面的，常常跨越软件生存期的各个阶段。所有这些方面都应逐步建立标准或规范。软件工程标准化的主要内容包括过程标准（如方法、技术和度量等）、产品标准（如需求、设计、部件、描述、计划和报告等）、专业标准（如道德准则、认证等）、记法标准（如术语、表示法和语言等）、开发规范（如准则、方法和规程等）、文件规范（如文件范围、文件编制、文件内容要求和编写提示）、

维护规范（如软件维护、组织与实施等）以及质量规范（如软件质量保证、软件配置管理、软件测试和软件验收等）等。

我国于1983年5月成立了“计算机与信息处理标准化技术委员会”，下设13个分技术委员会，其中程序设计语言分技术委员会和软件工程技术委员会与软件相关。我国推行软件工程标准化工作的总原则是向国际标准靠拢，对于能够在我国适用的标准全部按等同采用的方法，以促进国际交流。虽然我国的软件工程标准化工作仍处于起步阶段，但在提高我国软件工程水平，促进软件产业的发展以及加强与国外的软件交流等方面必将起到应有的作用。现已得到国家批准的软件工程国家标准有下述4个标准。

1）基础标准

（1）信息处理：程序构造及其表示法的约定 GB/T 13502-92。

（2）信息处理系统：计算机系统配置图符号及其约定 GB/T 14085-93。

（3）软件工程术语标准 GB/T 11457-89。

（4）软件工程标准分类法 GB/T 15538-95。

2）开发标准

（1）软件开发规范 GB 8566-88。

（2）计算机软件单元测试 GB/T 15532-95。

（3）软件维护指南 GB/T 14079-93。

3）文档标准

（1）计算机软件产品开发文件编制指南 GB 8567-88。

（2）计算机软件需求说明编制指南 GB/T 9385-88。

（3）计算机软件测试文件编制指南 GB/T 9386-88。

4）管理标准

（1）计算机软件配置管理计划规范 GB/T 12505-90。

（2）计算机软件质量保证计划规范 GB/T 12504-90。

（3）计算机软件可靠性和可维护性管理 GB/T 14394-93。

（4）信息技术、软件产品评价、质量特性及其使用指南 GB/T 16260-96。

5.1.9 ISO 9000：2000 标准

ISO 9000 标准是一系列标准的统称。其质量管理模式为企业管理注入了新的活力和生机，给质量管理体系提供评价基础，为企业进行世界贸易带来质量可信度。ISO 9000过程方法的概念、顾客需求以及持续改进的思想贯穿于整个标准，把组织的质量管理体系满足顾客要求的能力和程度体现在标准的要求之中。ISO 9000：2000 标准的推出，标志着国际标准化活动已从名词术语、试验方法及产品质量三大传统领域迈向了管理体系的标准化与认证阶段。

ISO 9000：2000 族标准的构成如下。

（1）4 个核心标准，即 ISO 9000：2000《基本原理和术语》、ISO 9001：2000《质量管理体系一要求》、ISO 9004：2000《质量管理体系——业绩改进指南》和 ISO 9011：2000《质量和环境管理审核指南》。

（2）一个支持标准 ISO 10012《测量设备的质量保证要求》。

（3）6 个技术报告，即 ISO 10006《项目管理指南》、ISO 10007《技术状态管理指南》、ISO 10013《质量管理体系文件指南》、ISO 10014《质量经济性指南》、ISO 10015《教育和培训指南》和 ISO 10017《统计技术在 ISO 9001 中的应用指南》。

（4）三个小册子，即质量管理原理、选择和使用指南、小型企业的应用指南和一个技术规范。

5.1.10　能力成熟度模型

CMM 是 Carnegie Mellon 大学软件工程研究所（CMU / SEI）在与企业界和政府合作的基础上开发出来的模型。CMM 以几十年产品质量概念和软件工业的经验及教训为基础，为软件企业的软件能力不断走向成熟提供了有效的步骤和阶梯式的进化框架。它指明了一个成熟的软件企业在软件开发方面需要管理的主要工作，这些工作之间的关系，以及以怎样的先后次序一步一步地达到预定的目标，从而得到持续的过程改进，实现企业高效率、低成本地交付高质量软件产品的战略目标。

CMM 为软件企业的过程能力提供了一个阶梯式的进化框架，将软件过程改进的进化步骤组织成 5 个成熟度等级，每一个级别定义了一组过程能力目标，并描述了要达到这些目标应该采取的实践活动，为过程不断改进奠定了循序渐进的基础。第一级实际上是一个起点，任何准备按 CMM 体系进化的企业都自然处于这个起点上，并通过这个起点向第二级迈进。除第一级外，每一级都设定了一组目标，如果达到了这组目标，则表明达到了这个成熟级别，可以向下一个级别迈进。CMM 体系不主张跨越级别的进化，因为从第二级起，每一个低级别的实现均是高级别实现的基础。

（1）在初始级，企业一般缺少有效的管理，不具备稳定的软件开发与维护的环境。此时，软件过程是未加定义的随意过程，项目的执行是随意的甚至是混乱的，几乎没有定义过程的规则（或步骤）。软件过程在实际的工作过程中被经常改变（过程是随意的），其成果是不稳定的，不可预见的，不可重复的。也就是说，软件的计划、预算、功能和产品的质量都是不可确定和不可预见的。项目的成功完全依赖个人的能力和他们先前的经验、知识以及他们的进取心和积极程度。当项目遇到危机时，通常会放弃原定的计划而只专注于编程与测试。有些企业制定了一些软件工程规范，但这些规范未能覆盖基本的关键过程要求，并且在执行中没有政策、资源等方面的保证，因此它仍然被视为初始级。

（2）在可重复级，企业建立了基本的项目管理过程的政策和管理规程，对成本、进度和功能进行监控，以加强过程能力。对新项目的计划和管理是基于以往的相似或同类

项目的成功经验，以确保再一次的成功。一个可管理的过程则是一个可重复的过程，一个可重复的过程则能逐渐进化和成熟。这一级的重点集中在软件管理过程上，包括需求管理、项目管理、质量管理、配置管理和子合同管理等方面。软件项目的计划和跟踪与监控的稳定实施，表现出一个按计划执行的且阶段可控的软件开发过程，并表明软件开发过程是相对稳定的。过程建立在项目一级，项目的成功依赖于个人的能力以及管理层的支持。

（3）在定义级，企业全面采用综合性的管理及工程过程来管理，对整个软件生命周期的管理与工程化过程都已标准化，并综合成软件开发企业标准的软件过程。企业标准软件过程被证明是正确且实用的，所有开发的项目需根据标准过程，剪裁出与项目适宜的过程，并执行这些过程。企业标准软件过程被应用到所有的工程中，用于编制和维护软件。有的项目也可根据实际情况，对软件开发组织的标准软件过程进行剪裁。定义级建立了软件工程过程小组，长期承担评估与调整软件过程的任务，以适应未来软件项目的要求。企业内部的所有人对于所定义的软件过程的活动、任务有深入了解，以项目组的方式进行工作，形成产品团队。

（4）在管理级，企业开始定量地认识软件过程，软件质量管理和软件过程管理是量化的管理。对软件过程与产品质量建立了定量的质量目标，制定了软件过程和产品质量的详细而具体的度量标准，实现了度量标准化。通过一致的度量标准来指导软件过程，保证所有项目对生产率和质量进行度量，并作为评价软件过程及产品的定量基础。量化控制使得软件开发真正变成一种工业生产活动。软件过程按照明确的度量标准度量和操作，软件过程以及软件产品的质量的一些趋势就可以得到控制和预见。经度量后一旦发现质量超出或违反标准，可以采用一些方法及时改进。每个人都了解个人的作用与企业的关系，存在强烈的群体工作意识。

（5）在优化级，企业将会把工作重点放在对软件过程改进的持续性、预见及增强自身，防止缺陷及问题的发生，不断地提高过程处理能力上。通过来自过程执行的质量反馈和吸收新方法和新技术的定量分析来改善下一步的执行过程，即优化执行步骤，使软件过程能不断地得到改进。根据软件过程的效果，进行成本 / 利润分析，从成功的软件过程中吸取经验，把最好的创新成绩迅速向全企业转移；对失败的案例进行分析以找出原因并预先改进，把失败的教训告知全体组织以防止重复以前的错误，不断提高产品的质量和生产率。整个企业都存在自觉的、强烈的团队意识，每个人都致力于过程改进，力求减少错误率。

5.1.11 相关标准

计算机综合布线、计算机网络及系统集成方面的国家标准、行业标准以及企业标准主要如表 5-1 所示。

表 5-1　相关标准

序号	标 准 编 号	名　　称
1	20030191-T-339	数字域名规范
2	20032261-T-339	应用于无线 IP 技术的网络安全规范
3	20032279-T-339	因特网广告电子邮件格式要求
4	20051268-T-339	GB/T 17178.2-XXXX 信息技术 开放系统互连 一致性测试方法和框架 第 2 部分：抽象测试套规范
5	20051269-T-339	GB/T 17178.4-XXXX 信息技术 开放系统互连 一致性测试方法和框架 第 4 部分：测试实现
6	20051292-T-339	信息技术 开放系统互连 OSI 登记机构的操作规程 第 3 部分：ISO 和 ITU-T 管理的顶级弧下的对象标识符弧的登记
7	20060540-T-469	整合《信息技术 系统间的远程通信和信息交换 提供和支持 OSI 网络服务的协议组合 第 1 部分：一般原则》《信息技术 系统间的远程通信和信息交换 提供和支持 OSI 网络服务的协议组合 第 2 部分：提供和支持连接方式的网络服务》《信息技术 系统间的远程通信和信息交换 提供和支持 OSI 网络服务的协议组合 第 3 部分：提供和支持无连接方式的网络服务》
8	20060547-T-469	整合《信息技术 开放系统互连 局域网媒体访问控制（MAC）服务定义》《信息技术 系统间远程通信和信息交换 局域网和城域网 公共规范 第 1 部分：媒体访问控制（MAC）服务定义》
9	20061052-T-469	整合《信息处理系统 数据通信 高级数据链路控制平衡类规程 交换环境中数据链路层地址的决定/协商》《信息技术 系统之间的远程通信和信息交换 高级数据链路控制（HDLC）规程 通用 XID 帧信息字段内容和格式》《信息处理系统 数据通信 高级数据链路控制规程 规程类别汇编》《信息处理系统 数据通信 高级数据链路控制规程 帧结构》《数据通信 高级数据链路控制规程 规程要素汇编》
10	20061177-T-469	数据通信基本型控制规程
11	20061689-T-469	数据通信 DTE 提供定时的使用 X.24 互换电路的 DTE 到 DTE 物理连接
12	20061953-T-469	信息技术 开放系统互连 目录 第 1 部分：概念、模型和服务的概述
13	20061954-T-469	信息技术 开放系统互连 目录 第 2 部分：模型
14	20061955-T-469	信息技术 开放系统互连 目录 第 3 部分：抽象服务定义
15	20061956-T-469	信息技术 开放系统互连 目录 第 5 部分：协议规范
16	20061957-T-469	信息技术 开放系统互连 目录 第 6 部分：选择属性类型
17	20061958-T-469	信息技术 开放系统互连 目录 第 7 部分：选择客体类
18	20062178-T-469	信息技术 开放系统互连 公共管理信息服务定义
19	20062179-T-469	信息技术 开放系统互连 公共管理信息协议 第 1 部分：规范
20	20062200-T-469	信息技术 国际标准化轮廓的框架和分类方法 第 2 部分：OSI 轮廓用的原则和分类方法
21	20062202-T-469	信息处理系统 开放系统互连 联系控制服务元素服务定义
22	20062281-T-469	信息技术 系统间的远程通信和信息交换 X.25 DTE 一致性测试 第 3 部分：分组层一致性测试套
23	20062517-T-469	信息技术 开放系统互连 系统管理综述
24	20062523-T-469	信息技术 开放系统互连 分布式事务处理 第 1 部分：OSI TP 模型

续表

序号	标 准 编 号	名 称
25	20062524-T-469	信息技术 开放系统互连 分布式事务处理 第2部分：OSI TP 服务
26	20062525-T-469	信息技术 开放系统互连 分布式事务处理 第3部分：协议规范
27	20062607-T-469	信息处理 DTE/DCE 接口处起止式传输的信号质量
28	20062608-T-469	信息处理系统 数据通信 高级数据链路控制规程 与X.25 LAPB 兼容的DTE数据链路规程的描述
29	20063114-T-469	信息处理 数据通信 使用25插针连接器的DTE/DCE 接口备用控制操作
30	20063115-T-469	信息处理系统 数据通信 网络服务定义
31	20063116-T-469	信息处理系统 数据通信 双扭线多点互连
32	20063117-T-469	信息处理系统 开放系统互连 面向连接的基本会话服务定义
33	20063205-T-469	信息处理系统 开放系统互连 运输服务定义
34	20063209-T-469	信息处理系统 开放系统互连 面向连接的运输协议规范
35	20063454-T-469	信息处理系统 局域网 第2部分：逻辑链路控制
36	20063455-T-469	信息处理系统 局域网 第3部分：带碰撞检测的载波侦听多址访问（CSMA/CD）的访问方法和物理层规范
37	20063478-T-469	信息处理系统 开放系统互连 面向连接的表示服务定义
38	20063530-T-469	数据通信 37插针及9插针 DTE/DCE 接口连接器和插针分配
39	20063531-T-469	数据通信 34插针 DTE/DCE 接口连接器和插针分配
40	20063532-T-469	数据通信 15插针 DTE/DCE 接口连接器和插针分配
41	20063817-T-469	信息处理系统 开放系统互连 基本参考模型 第3部分：命名与编址
42	20064290-T-469	信息技术 局域网和城域网 第5部分：令牌环访问方法和物理层规范
43	20064298-T-469	信息处理系统 开放系统互连 面向连接的表示协议规范
44	20064324-T-469	信息技术 国际标准化轮廓的框架和分类方法 第1部分：框架
45	20064442-T-469	信息技术 开放系统互连 目录 第4部分：分布式操作规程
46	20064553-T-469	信息处理系统 开放系统互连 联系控制服务元素协议规范
47	20064585-T-469	信息技术 系统间的远程通信和信息交换 X.25 DTE 一致性测试 第2部分：数据链路层一致性测试套
48	20064673-T-469	信息技术 提供无连接方式网络服务的协议 第1部分：协议规范
49	20064697-T-469	数据通信 使用V.24和X.24互换电路的DTE到DTE物理连接的接法
50	20070005-T-469	信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 无线高速率超宽带物理层和媒体访问控制规范
51	20070006-T-469	信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 无线高速率超宽带物理层和媒体访问接口规范
52	20070007-T-469	信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第15.4部分：低速率无线个域网（WPAN）物理层和媒体访问控制层规范
53	20070008-T-469	信息技术 开放系统互连 对象标识符（OID）的国家编号体系和注册规程
54	20075429-T-469	GB/T 17178.6-XXXX 信息技术 开放系统互连 一致性测试方法和框架 第6部分：协议轮廓测试规范
55	20075437-T-469	测试描述方法（MTS)；测试和测试控制表示法 第三版；第一部分：TTCN-3核心语言

续表

序号	标准编号	名称
56	20075464-T-469	基于联邦模型的 P2P 网络管理方法
57	20075519-T-469	无线局域网测评规范
58	20075590-T-469	信息技术 报文处理系统（MHS） 第 10 部分：MHS 路由选择
59	20075591-T-469	信息技术 报文处理系统（MHS） 第 8 部分：电子数据交换报文服务
60	20075592-T-469	信息技术 报文处理系统（MHS） 第 9 部分：电子数据交换报文系统
61	20075602-T-469	信息技术 计算机图形和图像处理 扩充 3D（X3D） 第 1 部分：体系结构和基础部件
62	20075603-T-469	信息技术 家用通用布缆
63	20075605-T-469	信息技术 开放系统互连 OSI 注册机构操作规程：唯一标识符（UUID）的生成和注册及其作为 ASN.1 客体标识符部件的使用
64	20075606-T-469	信息技术 开放系统互连 一致性测试方法和框架 第 5 部分：测试实验室和客户关于一致性评定过程的要求
65	20075625-T-469	信息技术 用户建筑群的路径和间隔

《综合布线国家标准 GBT-T 2050311-2000》从系统设计、系统指标、工作区、配线子系统、干线子系统、设备间、管理、 建筑群子系统、电气防护、接地及防火以及安装工艺要求对计算机布线系统进行了详尽地规范和指定。为了适应经济建设高速发展和改革开放的社会需求，配合现代化城市建设和信息通信网向数字化、综合化、智能化方向发展，搞好建筑与建筑群的电话、数据、图文和图像等多媒体综合网络建设，特制定综合布线国家标准规范。本规范适用于新建、扩建、改建建筑与建筑群的综合布线系统工程设计。综合布线系统的设施及管线的建设，应纳入建筑与建筑群相应的规划之中。综合布线系统应与大楼办公自动化（OA）、通信自动化（CA）和楼宇自动化（BA）等系统统筹规划，按照各种信息的传输要求做到合理使用，并应符合相关的标准。工程设计时，应根据工程项目的性质、功能、环境条件和近、远用户要求进行综合布线系统设施和管线的设计。工程设计施工必须保证综合布线系统的质量和安全，考虑施工和维护方便，做到技术先进，经济合理。工程设计中必须选用符合国家有关技术标准的定型产品。未经国家认可的产品质量监督检验机构鉴定合格的设备及主要材料，不得在工程中使用。综合布线系统的工程设计，除应符合本规范外，尚应符合国家现行的相关强制性标准的规定。建筑与建筑群综合布线系统（generic cabling system for building and campus）是指建筑物或建筑群内的传输网络。它既使话音和数据通信设备、交换设备和其他信息管理系统彼此相连，又使这些设备与外部通信网络相连接。它包括建筑物到外部网络或电话局线路上的连线点与工作区的话音或数据终端之间的所有电缆及相关联的布线部件。

目前在国内广泛使用的综合布线标准是美国的 EIA-568A、EIA-568B。

《数字域名系统国家标准 SJT 11271-2002》从数字域名系统、数字域名的扩展、数字域名与 IP 地址的映射以及标准的实施等几个方面对数字域名系统进行了规范。主要规定了数字域名的结构、语法以及数字域名与网络地址（主要是 IP 地址）之间的映射机制，

同时规定了数字域名标准的实施要求。本规范适用于因特网的数字域名的命名、系统运行和系统实现。

计算机信息系统集成通常称为计算机系统集成，简称系统集成。在系统集成方面，国家暂时没有出台相应的国家标准。1999 年，信息产业部颁发的《计算机信息系统集成资质管理办法（试行）》第二条指出，计算机信息系统集成是指从事计算机应用系统工程和网络系统工程总体策划、设计、开发、实施、服务及保障。早期的“系统集成”技术主要包括计算机和网络设备软硬件安装和测试、网络布线和测试以及防火、防雷击、防静电等物理安全。发展至今，“系统集成”技术主要包括以下几个方面：系统解决方案；软件系统开发；各子系统之间的集成；信息系统安全等。按照信息产业部《计算机信息系统集成资质管理办法（试行）》的规定，计算机信息系统集成包括总体策划、设计、开发、实施、服务及保障全过程。由于系统集成包含的内容太广泛，暂无国家标准，但随着整个社会信息化以及电子政务的发展，系统集成在 IT 行业中占有很大比重且发展迅速，各部门为了促进本行业信息化的发展，纷纷先于国家标准而制定了本部门的信息系统集成标准。如国家环保总局发布的《环境信息系统集成技术规范 HJ/T 418-2007》，从总体框架、应用集成、数据集成以及网络集成等几个方面对环境信息系统的建设进行了较为详尽地规范。

5.2 知识产权

5.2.1 知识产权的概念与特点

1．知识产权的概念

知识产权是人们基于自己的智力活动创造的成果和经营管理活动中的经验、知识而依法享有的权利。《中华人民共和国民法通则》规定，知识产权是指民事权利主体（公民、法人）基于创造性的智力成果。知识产权可分为工业产权和著作权。

（1）工业产权。根据保护工业产权巴黎公约第一条的规定，工业产权包括专利、实用新型、工业品外观设计、商标、服务标记、厂商名称、产地标记或原产地名称、制止不正当竞争等项内容。此外，商业秘密、微生物技术和遗传基因技术等也属于工业产权保护的对象。对于工业产权保护的对象，可以分为创造性成果权利和识别性标记权利。发明、实用新型和工业品外观设计等为创造性成果权利，它们的智力创造的表现比较明显，发明和实用新型是利用自然规律做出的解决特定问题的新的技术方案，工业品外观设计是确定工业品外表的美学创作，完成人需要付出创造性劳动。商标、服务标记、厂商名称、产地标记或原产地名称以及《中华人民共和国反不正当竞争法》第五条规定的知名商品特有的名称、包装和装潢等为识别性标记权利。

（2）著作权。著作权（也称为版权）是指作者对其创作的作品享有的人身权和财产

权。人身权包括发表权、署名权、修改权和保护作品完整权等。财产权包括作品的使用权和获得报酬权，即以复制、表演、播放、展览、发行、摄制电影、电视、录像或者改编、翻译、注释、编辑等方式使用作品的权利，以及许可他人以上述方式使用作品并由此获得报酬的权利。著作权保护的对象包括文学、科学和艺术领域内的一切作品，不论其表现形式或方式如何，诸如书籍、小册子和其他著作；讲课、演讲和其他同类性质作品；戏剧或音乐作品；舞蹈艺术作品和哑剧作品；配词或未配词的乐曲；电影作品以及与使用电影摄影艺术类似的方法表现的作品；图画、油画、建筑、雕塑、雕刻和版画；摄影作品以及使用与摄影艺术类似的方法表现的作品；与地理、地形建筑或科学技术有关的示意图、地图、设计图和草图等。

2．知识产权的特点

（1）无形性。知识产权的客体指的是智力创作性成果（也称为知识产品），是一种没有形体的精神财富。

（2）双重性。某些知识产权具有财产权和人身权双重性。例如著作权，其财产权属性主要体现在所有人享有的独占权以及许可他人使用而获得报酬的权利，所有人可以通过独自实施获得收益，也可以通过有偿许可他人实施获得收益，还可以像有形财产那样进行买卖或抵押；其人身权属性主要是指署名权等。有的知识产权具有单一的属性，例如，发现权只具有名誉权属性，不具有财产权属性；商业秘密只具有财产权属性，不具有人身权属性等。

（3）确认性。无形的智力创作性成果不像有形财产那样直观可见，因此，确认智力创作性成果的财产权需要依法审查确认得到法律保护。例如，发明人所完成的发明创造，其实用新型或者外观设计已经具有价值和使用价值。但是，其完成人尚不能自动获得专利权，必须依照《中华人民共和国专利法》的有关规定，向国家专利局提出专利申请，专利局依照法定程序进行审查，申请符合专利法规定条件的，由专利局做出授予专利权的决定，颁发专利证书，只有当专利局发布授权公告后，其完成人才享有该项知识产权。又如商标权的获得，我国实行注册制，只有向国家商标局提出注册申请，经审查核准注册后，才能获得商标权。

（4）独占性。由于智力成果具有可以同时被多个主体所使用的特点，因此，法律授予知识产权一种专有权，即具有独占性。未经其权利人许可，任何单位或个人不得使用，否则就构成侵权，并承担相应的法律责任。法律对各种知识产权都规定了一定的限制条件，但这些限制条件不影响其独占性特征。少数知识产权不具有独占性特征。例如，技术秘密的所有人不能禁止第三人使用其独立开发完成的或者合法取得的相同技术秘密。

（5）地域性。知识产权具有严格的地域性特点，即各国主管机关依照其本国法律授予的知识产权，只能在其本国领域内受法律保护。例如，中国专利局授予的专利权或中国商标局核准的商标专用权，只能在中国领域内受保护，其他国家则不给予保护，外国人在我国领域外使用中国专利局授权的发明专利，不侵犯我国专利权。著作权虽然自动

产生，但它受地域限制。我国法律对外国人的作品并不是都给予保护，只保护共同参加国际条约国家的公民的作品。同样，公约的其他成员国也按照公约规定，对我国公民和法人的作品给予保护。

（6）时间性。知识产权具有法定的保护期限，一旦保护期限届满，权利将自行终止，成为社会公众可以自由使用的知识。至于期限的长短，依各国的法律确定。例如，我国发明专利的保护期为20年，实用新型专利权和外观设计专利权的期限为10年，均自专利申请日起计算。我国公民的作品发表权的保护期为作者终生及其死亡后50年。我国商标权的保护期限自核准注册之日起10年，但可以根据其所有人的需要无限地续展权利期限，在期限届满前6个月内申请续展注册，每次续展注册的有效期为10年，续展注册的次数不限。如果商标权人逾期不办理续展注册，则其商标权也将终止。商业秘密受法律保护的期限是不确定的，该秘密一旦被公众所知悉，即成为公众可以自由使用的知识。

5.2.2 计算机软件著作权的主体与客体

1．计算机软件著作权的主体

计算机软件著作权的主体是指享有著作权的人。计算机软件著作权的主体包括公民、法人和其他组织。

（1）公民取得软件著作权主体资格的途径包括：公民自行独立开发软件（软件开发者）；订立委托合同，委托他人开发软件，并约定软件著作权归自己享有；通过转让取得软件著作财产权主体资格（软件权利的受让者）；合作开发计算机软件而产生的公民群体或者公民与其他主体成为计算机软件作品的著作权人；根据《中华人民共和国继承法》的规定通过继承取得软件著作财产权主体资格。

（2）法人取得计算机软件著作权主体资格一般通过的途径有：由法人组织并提供创作物质条件所实施的开发，并由法人承担社会责任；通过接受委托、转让等各种有效合同关系而取得著作权主体资格；因计算机软件著作权主体（法人）发生变更而依法成为著作权主体。

（3）其他组织是指除去法人以外的能够取得计算机软件著作权的其他民事主体，包括非法人单位、合作伙伴等。

2．计算机软件著作权的客体

计算机软件著作权的客体是指著作权法保护的计算机软件著作权的范围（受保护的对象）。著作权法保护的计算机软件是指计算机程序（源程序和目标程序）及其有关文档（程序设计说明书、流程图和用户手册等）。

5.2.3 计算机软件受著作权法保护的条件

1．独立创作

受保护的软件必须由开发者独立开发创作，任何复制或抄袭他人开发的软件不能获

得著作权。一个程序的功能设计往往被认为是程序的思想概念，根据著作权法不保护思想概念的原则，任何人可以设计具有类似功能的另一件软件作品。

2．可被感知

受著作权法保护的作品应当是固定在载体上的作者创作思想的一种实际表达。如果作者的创作思想未表达出来不可以被感知，就不能得到著作权法的保护。因此，《计算机软件保护条例》规定，受保护的软件必须固定在某种有形物体上，如固定在存储器或磁盘、磁带等计算机外部设备上，也可以是其他的有形物，如纸张等。

3．逻辑合理

计算机运行过程实际上是按照预先安排不断对信息随机进行的逻辑判断智能化过程。逻辑判断功能是计算机系统的基本功能。受著作权法保护的计算机软件作品必须具备合理的逻辑思想，并以正确的逻辑步骤表现出来。

5.2.4　计算机软件著作权的权利

软件作品享有两类权利：一类是软件著作权的人身权（精神权利），另一类是软件著作权的财产权（经济权利）。

1．软件著作权的人身权

软件著作权人享有的发表权和开发者身份权，是软件著作权人的人身权不可分离的主体。

（1）发表权是指决定软件作品是否公之于众的权利，即指软件作品完成后，以复制、展示、发行或翻译等方式使软件作品公之于众，或者在一定数量不特定人的范围内公开。发表权的具体内容包括软件作品发表的时间、发表的形式以及发表的地点等。

（2）开发者身份权是指作者为表明身份在软件作品上署上自己名字的权利。署名可有多种形式，既可以署作者的姓名，也可以署作者的笔名，或者作者自愿不署名。作品的署名对确认著作权的主体具有重要意义。身份权不随软件开发者的消亡而丧失，而且无时间限制。

2．软件著作权的财产权

财产权是指能够给著作权人带来经济利益的权利。财产权通常是指由软件著作权人控制和支配，并能够为权利人带来一定经济效益的权利内容。软件著作权人享有下述软件财产权。

（1）使用权。使用权是在不损害社会公共利益的前提下，以复制、修改、发行、翻译和注释等方式合作软件的权利。

（2）复制权。复制是将软件作品制作一份或多份的行为。复制权就是版权所有人决定实施或不实施上述复制行为或者禁止他人复制其受保护作品的权利。

（3）修改权。修改是对软件进行增补、删节，或者改变指令、语句顺序等以提高、完善原软件作品的做法。修改权即指作者享有的修改或者授权他人修改软件作品的权利。

（4）发行权。发行权是指为满足公众的合理需求，通过出售、出租或者赠与等方式向公众提供软件的原件或者一定数量的软件作品复制件的权利。

（5）翻译权。翻译是指以不同于原软件作品的一种程序语言转换该作品原使用的程序语言，而重现软件作品内容的创作。简单地说，翻译权就是指将原软件从一种程序语言转换成另一种程序语言的权利。

（6）注释权。软件作品的注释是指对软件作品中的程序语句进行解释，以便更好地理解软件作品。注释权是指著作权人对自己的作品享有进行注释的权利。

（7）信息网络传播权。即以有线或者无线信息网络方式向公众提供软件作品，使公众可在其个人选定的时间和地点获得软件作品的权利。

（8）出租权。即有偿许可他人临时使用计算机软件的复制件的权利，但是，计算机软件不是出租的主要标的的除外。

（9）使用许可权和获得报酬权。即许可他人以上述方式使用软件作品的权利（许可他人行使软件著作权中的财产权）和依照约定或者法律有关规定获得报酬的权利。

（10）转让权。即向他人转让软件的使用权和使用许可权的权利。软件著作权人可以全部或者部分转让软件著作权中的财产权。

3．软件合法持有人的权利

根据《计算机软件保护条例》的规定，软件的合法复制品所有人享有下述权利。

（1）根据使用的需要把软件装入计算机等具有信息的装置内。

（2）根据使用的需要而进行必要的复制。

（3）为了防止复制品损坏而制作备份复制品，这些复制品不得通过任何方式提供给他人使用，并在所有人丧失该合法复制品所有权时，负责将备份复制品销毁。

（4）为了把该软件用于实际的计算机应用环境或者改进其功能性能而进行必要的修改。但是，除合同约定外，未经该软件著作权人许可，不得向任何第三方提供修改后的软件。

5.2.5 计算机软件著作权的行使

1．软件经济权利的许可使用

软件经济权利的许可使用是指软件著作权人或权利合法受让者，通过合同方式许可他人使用其软件并获得报酬的一种软件贸易形式。许可使用的方式可分为以下几种。

（1）独占许可使用：权利人通过书面合同授权，被授权方可以根据合同规定的方式、条件、时间确定独占性，权利人不得将软件使用权授予第三方，权利人自己不能使用该软件。

（2）独家许可使用：权利人通过书面合同授权，被授权方可以根据合同规定的方式、条件、时间确定独占性，权利人不得将软件使用权授予第三方，权利人自己可以使用该软件。

（3）普通许可使用：权利人通过书面合同授权，被授权方可以根据合同规定的方式、条件、时间确定独占性，权利人可以将软件使用权授予第三方，权利人自己可以使用该软件。

（4）法定许可使用和强制许可使用：在法律特定的条款下，不经软件著作权人许可，使用其软件。

2．软件经济权利的转让使用

软件经济权利的转让使用是指软件著作权人将其享有的软件著作权中的经济权利全部转移给他人。软件经济权利的转让将改变软件权利的归属，原始著作权人的主体地位随着转让活动的发生而丧失，软件著作权受让者成为新的著作权主体。软件著作权转让必须签订书面合同。软件转让活动不能改变软件的保护期。转让方式包括出卖、赠与、质押和赔偿等。

5.2.6　计算机软件著作权的保护期

根据《中华人民共和国著作权法》和《计算机软件保护条例》的规定，计算机软件著作权的权利自软件开发完成之日起产生，公民的软件著作权，保护期为公民终生及其死亡之后 50 年；法人或其他组织的软件著作权，保护期为 50 年。保护期满，除开发者身份权以外，其他权利终止。一旦计算机软件著作权超出保护期后，软件进入公有领域。计算机软件著作权人的单位终止和计算机软件著作权人的公民死亡均无合法继承人的，除开发者身份权以外，该软件的其他权利进入公有领域。软件进入公有领域后成为社会公共财富，公众可无偿使用。

5.2.7　计算机软件著作权的归属

1．职务开发软件著作权的归属

职务软件作品是指公民在单位任职期间为执行本单位工作任务所开发的计算机软件作品。本单位工作任务的含义，一是指该软件系为其本职工作明确指定的目标而开发；二是指该软件的开发系其从事本职工作完成工作任务能够预见或必然的结果，或者主要使用了单位的专用设备、未公开的专门信息等物资技术条件所开发并由法人或者其他组织承担责任的软件。根据《计算机软件保护条例》的规定，可以得出这样的结论：当公民作为某单位的雇员时，如其开发的软件属于执行本职工作的结果，该软件著作权应当归单位享有；所开发的软件如不是执行本职工作的结果，其著作权就不属单位享有；如果该雇员主要使用了单位的设备，按照《计算机软件保护条例》第十三条第三款的规定，其著作权不能属于该雇员个人享有。

对于公民在非职务期间创作的计算机程序，其著作权是属于某项软件作品的开发单位，还是从事直接创作开发软件作品的个人，可按照《计算机软件保护条例》第十三条规定的三条标准确定。

（1）任何受雇于一个单位的人员，都会被安排一定的工作岗位和分派相应的工作任务。其完成分派的工作任务，就是执行他的本职工作。本职工作的直接成果也就是其工作任务的不断完成。当然，具体工作成果又会产生许多效益，产生许多范围更广的结果。但是区别该条标准应当是指雇员本职工作最直接的成果。所开发创作的软件不是执行本职工作的结果，这也是构成非职务计算机软件著作权的条件之一。

（2）如果该雇员在单位担任软件开发工作，引起争议的软件作品不能与其本职工作中明确指定的开发目标有关，软件作品的内容也不能与其本职工作所开发的软件的功能、逻辑思维和重要数据有关。雇员所开发的软件作品与其本职工作没有直接的关系是构成非职务计算机软件著作权的条件之二。

（3）开发创作软件作品所使用的物质技术条件，即开发软件作品所必须的设备、数据、资金和其他软件开发环境。没有使用受雇单位的任何物质技术条件是构成非职务软件著作权的第三个条件。

雇员进行本职工作以外的软件开发创作，必须同时符合上述三个条件，才能算是非职务软件作品，雇员个人才享有软件著作权。常有软件开发符合前两个条件，但使用了单位的技术情报资料、计算机设备等物质技术条件的情况。处理此种情况较好的方法是对该软件著作权的归属应当由单位和雇员双方协商确定，如对于公民在非职务期间利用单位物质条件创作的与单位业务范围无关的计算机程序，其著作权属于创作程序的作者，但作者许可第三人使用软件时，应当支付单位合理的物质条件使用费，如计算机机时费等。若协商不能解决，只能按上述三条标准作出界定。

2．合作开发软件著作权的归属

合作开发软件是指两个或两个以上公民、法人或其他组织订立协议，共同参加某项计算机软件的开发并分享软件著作权的形式。

（1）由两个以上的单位、公民共同开发完成的软件属于合作开发的软件。对于合作开发的软件，其著作权的归属一般是由各合作开发者共同享有。但如果有软件著作权的协议，则按照协议确定软件著作权的归属。

（2）对于合作开发的软件著作权无书面合同或者合同未作明确约定，合作开发的软件可以分割使用的，开发者对各自开发的部分可以单独享有著作权，但是，行使著作权时，不得扩展到合作开发的软件整体的著作权。合作开发的软件不能分割使用的，其著作权由合作开发者共同享有，通过协商一致行使。如不能协商一致，又无正当理由，任何一方不得阻止他方行使除转让权以外的其他权利，但是所得收益应合理分配给所有合作开发者。

（3）合作开发者对于软件著作权中的转让权项不得单独行使。这是因为转让权的行使将涉及软件著作权权利主体的改变，所以合作软件的开发者在行使转让权时，必须与各合作开发者协商，在征得同意的情况下方能行使该项专有权利。

3．委托开发的软件著作权归属

委托开发软件著作权关系的建立，一般由委托方与受委托方订立合同而成立。委托开发软件作品关系中，委托方的责任主要是提供资金、设备等物质条件，并不直接参与开发软件作品的创作开发活动，受托方的主要责任是根据委托合同规定的目标开发出符合要求的软件。委托开发软件作品系根据委托方的要求，由委托方与受托方以合同确定的权利和义务的关系而进行开发的软件。因此，软件作品著作权归属应当作为合同的重要条款予以明确约定。对于在委托开发软件活动中，委托者与受委托者没有签订书面协议，或者在协议中未对软件著作权归属作出明确的约定，其软件著作权属于受委托者，即属于实际完成软件的开发者。

4．接受任务开发的软件著作权归属

根据社会经济发展的需要，对于一些涉及国家基础项目或者重点设施的计算机软件，往往采取由政府有关部门或上级单位下达任务方式，完成软件的开发工作。对于下达任务开发的软件，其著作权的归属关系如下。

（1）下达任务开发的软件著作权的归属关系，首先应以项目任务书的规定或者双方的合同约定为准确定。

（2）下达任务的项目任务书或者双方订立的合同中未对软件著作权归属作出明确的规定或者约定的，其软件著作权属于接受并实际完成开发软件任务的单位享有。

5．计算机软件著作权主体变更后软件著作权的归属

计算机软件著作权的主体，因一定的法律事实而发生变更，如作为软件著作权人的公民的死亡，单位的变更，软件著作权的转让以及人民法院对软件著作权的归属作出裁判等。软件著作权主体的变更必然引起软件著作权归属的变化，对此，《计算机软件保护条例》作了一些规定。因计算机软件主体变更引起的权属变化有以下几种。

（1）软件著作权的合法继承人依法享有继承被继承人享有的软件著作权的使用权、使用许可权和获得报酬权等权利。继承权的取得、继承顺序等均按照《中华人民共和国继承法》的规定进行。

（2）作为软件著作权人的单位发生变更（如单位的合并、破产等），而其享有的软件著作权仍处在法定的保护期限内，可以由合法的权利承受单位享有原始著作权人所享有的各项权利。依法承受软件著作权的单位成为该软件的后续著作权人，可在法定的条件下行使所承受的各项专有权利。一般认为，“各项权利”包括署名权等著作人身权在内的全部权利。

6．权利转让后软件著作权的归属

计算机软件著作财产权发生转让后，必然引起著作权主体的变化，产生新的软件著作权归属关系。软件权利的受让者可依法行使其享有的权利。

7．司法判决、裁定引起的软件著作权归属问题

计算机软件著作权是公民、法人和其他组织享有的一项重要的民事权利。当发生争

议和纠纷后由人民法院的民事判决、裁定而产生软件著作权主体的变更，引起软件著作权归属问题。因司法裁判引起软件著作权的归属问题主要有如下4类。

（1）由人民法院对著作权属纠纷中权利的最终归属作出司法裁判，从而变更了计算机软件著作权原有归属。

（2）计算机软件的著作权人为民事法律关系中的债务人（债务形成的原因可能多种多样，如合同关系或者损害赔偿关系等），人民法院将其软件著作财产权判归债权人享有抵债。

（3）人民法院作出民事判决判令软件著作权人履行民事给付义务，在判决生效后执行程序中，其无其他财产可供执行，将软件著作财产权执行给对方折抵债务。

（4）根据《中华人民共和国破产法》的规定，软件著作权人被破产还债，软件著作财产权为法律规定的破产财产构成的“其他财产权利”，作为破产财产由人民法院判决分配。

8．保护期限届满权利丧失

软件著作权的法定保护期限可以确定计算机软件的主体能否依法变更。如果软件著作权已过保护期，该软件进入公有领域，便丧失了专有权，也就没有必要改变权利主体了。

5.2.8 计算机软件著作权侵权的鉴别

侵犯计算机软件著作权的违法行为的鉴别，主要依靠保护知识产权的相关法律来判断。违反《中华人民共和国著作权法》、《计算机软件保护条例》等法律禁止的行为，便是侵犯计算机著作权的违法行为，这是鉴别违法行为的本质原则。对于法律规定不禁止，也不违反相关法律基本原则的行为，不认为是违法行为。在法律无明文具体条款规定的情况下，违背《中华人民共和国著作权法》和《计算机软件保护条例》等法律的基本原则，以及社会主义公共生活准则和社会善良风俗的行为，也应该视为违法行为。凡是行为人主观上具有故意或者过失对《中华人民共和国著作权法》和《计算机软件保护条例》保护的计算机软件人身权和财产权实施侵害行为的，都构成计算机软件的侵权行为。《计算机软件保护条例》第二十三条规定的侵犯计算机软件著作权的情况，是认定软件著作权侵权行为的法律依据。计算机软件侵权行为主要有：

（1）未经软件著作权人的同意而发表或者登记其软件作品。

（2）将他人开发的软件当作自己的作品发表或者登记。

（3）未经合作者同意将与他人合作开发的软件当作自己独立完成的作品发表或者登记。

（4）在他人开发的软件上署名或者更改他人开发的软件上的署名。

（5）未经软件著作权人或者其合法受让者的许可，修改、翻译其软件作品。

（6）未经软件著作权人或其合法受让者的许可，复制或部分复制其软件作品。

（7）未经软件著作权人及其合法受让者同意，向公众发行、出租其软件的复制品。

（8）未经软件著作权人或其合法受让者同意，向任何第三方办理软件权利许可或转让事宜。

（9）未经软件著作权人及其合法受让者同意，通过信息网络传播著作权人的软件。

5.2.9　不构成计算机软件侵权的合理使用行为

获得使用权或使用许可权（视合同条款）后，可以对软件进行复制而无需通知著作权人，也不构成侵权。区分合理使用与非合理使用的判别标准一般如下。

（1）软件作品是否合法取得（这是合理使用的基础）。

（2）使用的目的是非商业营业性的，如果使用的目的是为商业性营利，就不属合理使用的范围。

（3）合理使用一般为少量的使用，所谓少量的界限，是根据其使用的目的以行业惯例和人们一般常识所综合确定。超过通常被认为的少量界限，即可被认为不属合理使用。

5.2.10　计算机软件著作权侵权的法律责任

当侵权人侵害他人的软件著作财产权或软件著作人身权，造成权利人财产上的或非财产的损失，侵权人不履行赔偿义务，法律即强制侵权人承担赔偿损失的民事责任。

1．民事责任

侵犯著作权或者与著作权有关的权利的，侵权人应当按照权利人的实际损失给予赔偿；实际损失难以计算的，可以按照侵权人的违法所得给予赔偿。赔偿数额还应当包括权利人为制止侵权行为所支付的合理开支。权利人的实际损失或侵权人的违法所得不能确定的，由人民法院根据侵权行为的情节，判决给予 50 万元以下的赔偿。有下列侵权行为的，应当根据情况，承担停止侵害、消除影响、公开赔礼道歉和赔偿损失等民事责任。

（1）未经软件著作权人许可发表或者登记其软件的。

（2）将他人软件当作自己的软件发表或者登记的。

（3）未经合作者许可，将合作开发的软件当作自己单独完成的作品发表或者登记的。

（4）在他人软件上署名或者涂改他人软件上的署名的。

（5）未经软件著作权人许可，修改、翻译其软件的。

（6）其他侵犯软件著作权的行为。

2．行政责任

对侵犯软件著作权的行为，著作权行政管理部门应当责令停止违法行为，没收非法所得，没收、销毁侵权复制品，并可处以每件 100 元或者货值金额 2～5 倍的罚款。有下列侵权行为的，应当根据情况，承担停止侵害、消除影响、公开赔礼道歉和赔偿损失等行政责任。

（1）复制或者部分复制著作权人软件的。

（2）向公众发行、出租、通过信息网络传播著作权人软件的。

（3）故意避开或者破坏著作权人为保护其软件而采取的技术措施的。

（4）故意删除或者改变软件权利管理电子信息的。

（5）许可他人行使或者转让著作权人的软件著作权的。

3．刑事责任

侵权行为触犯刑律的，侵权者应当承担刑事责任。《中华人民共和国刑法》第二百一十七条、二百一十八条和二百二十条规定，构成侵犯著作权罪、销售侵权复制品罪的，由司法机关追究其刑事责任。

5.2.11 计算机软件的商业秘密权

1．商业秘密的概念

《中华人民共和国反不正当竞争法》中将商业秘密定义为“不为公众所知悉的、能为权利人带来经济利益、具有实用性并经权利人采取保密措施的技术信息和经营信息”。经营秘密和技术秘密是商业秘密的基本内容。经营秘密，即未公开的经营信息，是指与生产经营销售活动有关的经营方法、管理方法、产销策略、货源情报、客户名单、标底和标书内容等专有知识。技术秘密，即未公开的技术信息，是指与产品生产和制造有关的技术诀窍、生产方案、工艺流程、设计图纸、化学配方和技术情报等专有知识。

商业秘密的构成条件是：必须具有未公开性，即不为公众所知悉；必须具有实用性，即能为权利人带来经济效益；必须具有保密性，即采取了保密措施。

商业秘密是一种无形的信息财产。商业秘密的权利人与有形财产所有权人一样，依法享有占有、使用和收益的权利，即有权对商业秘密进行控制与管理，防止他人采取不正当手段获取与使用；有权依法使用自己的商业秘密，而不受他人干涉；有权通过自己使用或者许可他人使用以至转让所有权，从而取得相应的经济利益；有权处分自己的商业秘密，包括放弃占有、无偿公开、赠与或转让等。

一项商业秘密受到法律保护的依据，是必须具备上述构成商业秘密的三个条件，缺少上述三个条件之一都会造成商业秘密丧失保护。

《中华人民共和国反不正当竞争法》保护计算机软件，是以计算机软件中是否包含着“商业秘密”为必要条件的。而计算机软件是人类知识、智慧、经验和创造性劳动的成果，本身就具有商业秘密的特征，即包含着技术秘密和经营秘密。即使是软件尚未开发完成，在软件开发中所形成的知识内容也可构成商业秘密。

2．计算机软件商业秘密的侵权

侵犯商业秘密是指行为人（负有约定的保密义务的合同当事人，实施侵权行为的第三人，侵犯本单位商业秘密的行为人）未经权利人（商业秘密的合法控制人）的许可，以非法手段（包括直接从权利人那里窃取商业秘密并加以公开或使用，通过第三人窃取权利人的商业秘密并加以公开或使用）获取计算机软件商业秘密并加以公开或使用的行

为。根据我国《中华人民共和国反不正当竞争法》第十条的规定，侵犯计算机软件商业秘密的具体表现形式主要如下。

（1）用盗窃、利诱、胁迫或其他不正当手段获取权利人的计算机软件商业秘密。盗窃商业秘密，包括单位内部人员、外部人员和内外勾结等盗窃手段；以利诱手段获取商业秘密，通常指行为人向掌握商业秘密的人员提供财物或其他优惠条件，诱使其向行为人提供商业秘密；以胁迫手段获取商业秘密，是指行为人采取威胁、强迫手段，使他人在受强制的情况下提供商业秘密；以及用其他不正当手段获取商业秘密。

（2）披露、使用或允许他人使用以不正当手段获取权利人的计算机软件商业秘密。披露是指将权利人的商业秘密向第三人透露或向不特定的其他人公开，使其失去秘密价值；使用或允许他人使用是指非法使用他人商业秘密的具体情形。如果以非法手段获取商业秘密的行为人将该秘密再行披露或使用，即构成双重的侵权；倘若第三人从侵权人那里获悉了商业秘密而将秘密披露或使用，同样构成侵权。

（3）违反约定或违反权利人有关保守商业秘密的要求，披露、使用或允许他人使用其所掌握的计算机软件商业秘密。合法掌握计算机软件商业秘密的人，可能是与权利人有合同关系的对方当事人，也可能是权利人的单位工作人员或其他知情人，他们违反合同约定或单位规定的保密义务，将其所掌握的商业秘密擅自公开，或自己使用，或许可他人使用，即构成侵犯商业秘密。

3．计算机软件商业秘密侵权的法律责任

根据《中华人民共和国反不正当竞争法》和《刑法》的规定，计算机软件商业秘密的侵权者将承担行政责任、民事责任以及刑事责任。

（1）《中华人民共和国反不正当竞争法》第二十五条规定了相应的行政责任，即对侵犯商业秘密的行为，监督检查部门应当责令停止违法行为，而后可以根据侵权的情节依法处以 1 万元以上 20 万元以下的罚款。

（2）计算机软件商业秘密的侵权者的侵权行为对权利人的经营造成经济上的损失时，侵权者应当承担经济损害赔偿的民事责任。《中华人民共和国反不正当竞争法》第二十条规定了侵犯商业秘密的民事责任，即经营者违反该法规定，给被侵害的经营者造成损害的，应当承担损害赔偿责任；被侵害的经营者的合法权益受到损害的，可以向人民法院提起诉讼。

（3）计算机软件商业秘密的侵权者的侵权行为对权利人造成重大损害的，侵权者应当承担刑事责任。《刑法》第二百一十九条规定了侵犯商业秘密罪，即实施侵犯商业秘密行为，给商业秘密的权利人造成重大损失的，处三年以下有期徒刑或者拘役，并处或者单处罚金；造成特别严重后果的，处三年以上七年以下有期徒刑，并处罚金。

第 6 章　网络系统分析与设计案例

网络规划师要求考生深入掌握网络系统所涉及的各种理论、技术以及网络系统设计方案和步骤。本部分的试题将给出若干方面的案例，参考人员应根据要求，完成相应的网络规划、网络优化、网络配置和网络排错工作。本章将围绕这 4 个方面给出一些案例进行分析和讲解。

6.1　网络规划案例

6.1.1　案例 1

某学校在原校园网的基础上进行网络改造，网络方案如图 6-1 所示。其中，网管中心位于办公楼第三层，采用动态及静态结合的方式进行 IP 地址的管理和分配。

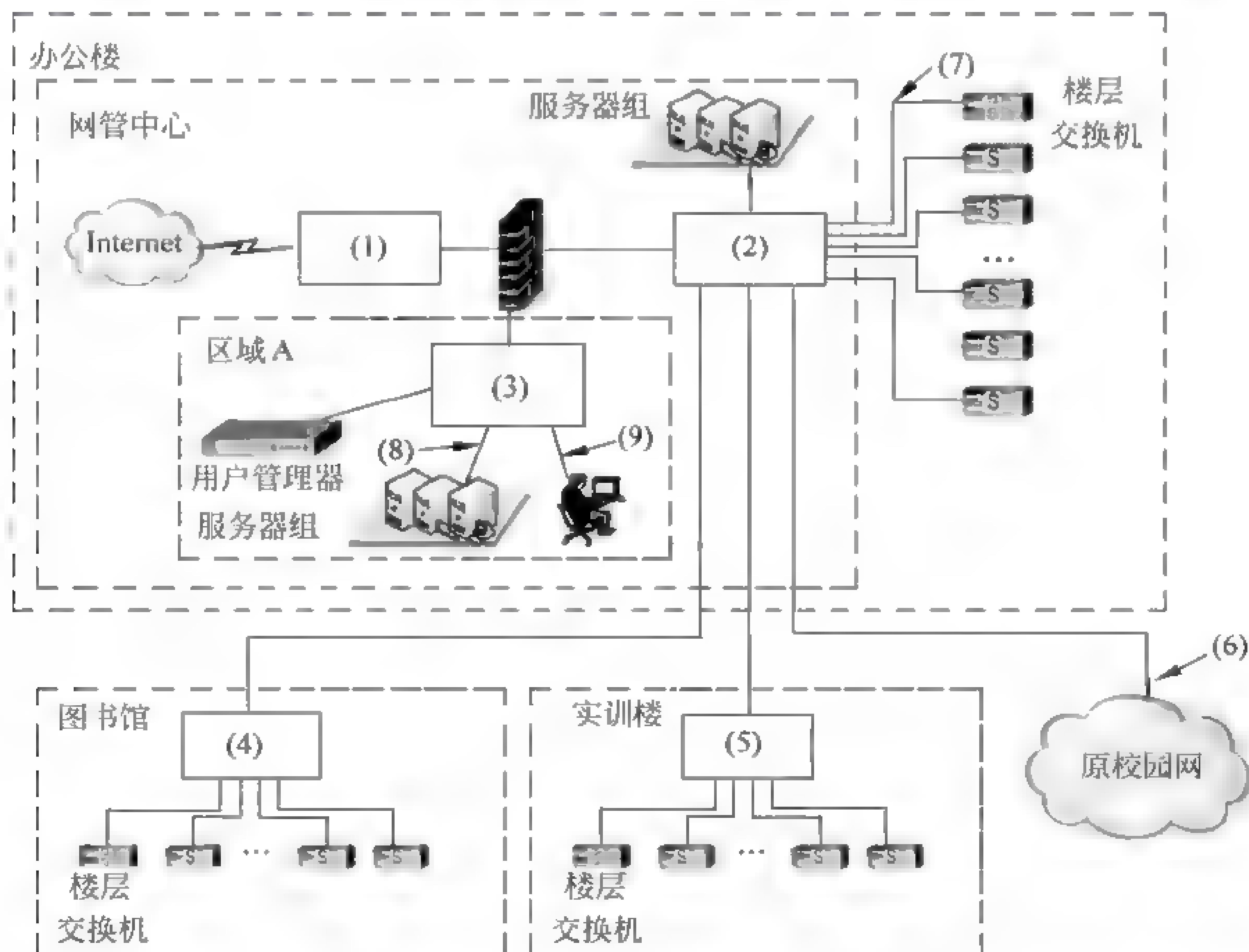


图 6-1　某校园网络改造方案

【问题 1】

设备选型是网络方案规划设计的一个重要方面，请用 200 字以内文字简要叙述设备选型的基本原则。

【问题 2】

从表 6-1 中为图 6-1 中（1）～（5）处选择合适设备，将设备名称写在答题纸的相应位置（每一设备限选一次）。

表 6-1　设备表

设备类型	设备名称	数量	性 能 描 述
路由器	Router1	1	模块化接入，固定的广域网接口+可选广域网接口，固定的局域网接口为 100/1000Base-T/TX
交换机	Switch1	1	交换容量：1.2TB，转发性能：285Mpps，可支持接口类型 100/1000Base-T、GE、10GE，电源冗余：1+1
	Switch2	1	交换容量：140GB，转发性能：100Mpps，可支持接口类型 GE，电源冗余：无，20 百/千兆自适应电口
	Switch3	2	交换容量：100GB，转发性能：66Mpps，可支持接口类型：FE、GE，电源冗余：无，24 千兆光口

【问题 3】

为图 6-1 中（6）～（9）处选择介质，填写在答题纸的相应位置。

备选介质（每种介质限选一次）：

千兆双绞线　　百兆双绞线　　双千兆光纤链路　　千兆光纤

【问题 4】

请用 200 字以内文字简要叙述针对不同用户分别进行动态和静态 IP 地址配置的优点，并说明图中的服务器以及用户采用哪种方式进行 IP 地址配置。

	IP 地址配置方式
邮件服务器	（1）
网管 PC	（2）
学生 PC	（3）

【问题 5】

通常有恶意用户采用地址假冒方式进行盗用 IP 地址，可以采用什么策略来防止静态 IP 地址的盗用？

【问题 6】

（1）图 6-1 中区域 A 是什么区？（请从以下选项中选择）

A. 服务区　　B. DMZ 区　　C. 堡垒主机　　D. 安全区

（2）学校网络中的设备或系统有存储学校机密数据的服务器、邮件服务器、存储资源代码的 PC、应用网关、存储私人信息的 PC 和电子商务系统等，这些设备哪些应放在

区域 A 中，哪些应放在内网中？请简要说明。

1．案例分析

（1）本案例问题 1 主要是考查网络设备选型方面的知识。一般而言，在选择网络设备时应当遵循以下原则。

- 可靠性：由于升级的往往是核心和骨干网络，其重要性不言而喻，一旦瘫痪则影响巨大。因此，必须将可靠性放在第一位，无论是品牌的选择还是设备的配置，都将可靠性作为第一考虑因素。
- 性能：作为骨干网络节点，中心交换机、会聚交换机必须能够提供完全无阻塞的多层交换性能，以保证业务的顺畅。
- 可管理性：一个中大型网络可管理程度的高低直接影响着运行成本和业务质量。因此，所有的节点都应是可网管的，而且需要有一个强有力且简洁的网络管理系统，能够对网络的业务流量、运行状况等进行全方位的监控和管理。
- 灵活性和可扩展性：由于校园网络结构复杂，需要交换机能够接续全系列接口，例如光口和电口、百兆、千兆和万兆端口，以及多模光纤接口和长距离的单模光纤接口等。其交换结构也应能根据网络的扩容灵活地扩大容量。其软件应具有独立知识产权，应保证其后续研发和升级以保证对未来新业务的支持。
- 安全性：随着网络的普及和发展，各种各样的攻击也在威胁着网络的安全。不仅仅是接入交换机，骨干层次的交换机也应考虑到安全防范的问题，例如访问控制、带宽控制等，从而有效控制不良业务对整个骨干网络的侵害。
- QoS 控制能力：随着网络上多媒体业务流（语音、视频等）越来越多，对核心交换节点提出了更高的要求，不仅要能进行一般的线速交换，还要能根据不同业务流的特点，对它们的优先级和带宽进行有效的控制，从而保证重要业务和时间敏感业务的顺畅。
- 标准性和开放性：由于网络往往是一个具有多种厂商设备的环境，因此，所选择的设备必须能够支持业界通用的开放标准和协议，以便能够和其他厂商的设备有效地互通。
- 性价比：在满足网络需求和网络应用的基础上，还应当充分考虑设备的性价比，以达到最大的投资回报率。

（2）问题 2 要求考生掌握网络方案设计中设备部署的相关知识，从表 6-1 中关于路由器设备的性能描述“固定的广域网接口+可选广域网接口”可知，图 6-1 中空（1）处的网络设备应选择路由器（Router1）。通过 Router1 的广域网接口连接到 Internet。根据交换容量、包转发能力、可支持接口类型和电源冗余模块等方面对比表 6-1 中交换机设备 Switch1、Switch2、Switch3 可知，设备 Switch1 的性能和可靠性最好，设备 Switch2 的性能次之，设备 Switch3 的性能稍差一些。仔细分析该校园网的拓扑结构，可知空（2）处的网络设备是校园网的核心层，它必须提供稳定可靠的高速交换，并且能够连接各种

接口类型，因此空（2）处的设备应为 Switch1。

空（3）处的网络设备至少需要提供一个百兆/千兆电口用于连接至防火墙的 DMZ 接口，若干个快速以太网电口或光口用于连接服务器组、用户管理器和网络管理工作站。表 6-1 中关于交换机设备 Switch2 的性能描述“可支持接口类型：GE，20 百/千兆自适应电口”信息可满足以上网络连接要求，因此空（3）处的网络设备应选择交换机 Switch2。

从空（4）和空（5）的位置可知，该设备位于汇聚层。考虑到综合布线系统中各大楼建筑物之间通常采用光纤作为传输介质，结合表 6-1 中关于交换机设备 Switch3 的性能描述“可支持接口类型：FE、GE，24 千兆光口”信息可知，空（4）和空（5）处的网络设备应选择交换机 Switch3。

（3）问题 3 要求考生掌握网络方案设计中传输介质选择的相关知识。

由 IEEE 802.3ad 工作组制定的链路聚合（Port Trunking）技术，支持 IEEE 802.3 协议，是一种用来在两台核心交换机之间扩大通信吞吐量、提高可靠性的技术。该技术可使交换机之间连接最多 4 条负载均衡的冗余连接。核心交换机之间采用双千兆光纤结构，可以保证在任何时刻任意一条链路出现故障时，在极短时间内自动切换到另一条链路上，从而排除单点故障。在图 6-1 拓扑结构中，新的核心层交换机与原校园网的连接介质应该采用双千兆光纤链路以提高可靠性。

结合工程经验可知，在层次化网络方案设计时，综合考虑到网络应用涉及到数据、音频、视频传输，为保证传输带宽和质量，核心层交换机与各楼层交换机的连接介质一般应采用千兆光纤，即空（7）处的传输介质可选择“千兆光纤”。

根据上面的分析可知，空（3）处的交换机 Switch2 可支持千兆以太网（GE）接口类型，且有 20 个百兆/千兆自适应电口。综合考虑到与 Switch2 交换机相连接的服务器组要求较高的通信性能，因此空（8）处的传输介质可选择“千兆双绞线”。空（9）处的传输介质用于连接网管工作站，一般与交换机设备距离不会超过 100m，并且对传输速率和服务质量没有太高要求，因此空（9）处的传输介质可选择“百兆双绞线”。

（4）本问题比较简单，一方面是考查静态 IP 地址和动态 IP 地址的区别，另一方面是考查哪些设备应配置静态 IP 地址，哪些设备适宜采用动态分配 IP 地址。

采用静态 IP 地址配置方案时，每个用户都有自己独立且固定的 IP 地址。通常企业网或校园网中的路由器、交换机、防火墙、各种应用服务器、网络管理工作站和网络打印机等应采用静态 IP 地址分配。因此本小题邮件服务器、网管 PC 需采用静态 IP 地址。

由于 IP 地址资源的宝贵性，加上用户上网时间和空间的离散性，采用动态 IP 地址配置方案为用户分配一个临时的 IP 地址，一方面可避免 IP 地址资源的浪费，另一方面对用户透明，不需要在每台用户计算机上配置 IP 参数，比较简单方便。这种配置方案增加了用户接入的灵活性，适合于客户机的接入场景，因此学生 PC 最好采用动态 IP 地址。

（5）本小题要求考生掌握防止静态 IP 地址盗用的相关知识。IP 地址的修改非常容易，而 MAC 地址存储在网卡的 EEPROM 中，而且网卡的 MAC 地址是唯一确定的。因

此，为了防止内部人员进行非法 IP 盗用（例如，盗用权限更高人员的 IP 地址，以获得权限外的信息），可以将内部网络的 IP 地址与 MAC 地址绑定，盗用者即使修改了 IP 地址，也因 MAC 地址不匹配而盗用失败。

（6）本小题要求考生掌握防火墙 DMZ 区概念以及服务器部署的相关知识。防火墙中的 DMZ 区也称为非武装区域，允许外网的用户有限度地访问其中的资源。通常，DMZ 区的安全规则如下。

① 允许外部网络用户访问 DMZ 区的面向外网的应用服务（如 Web、FTP 和 BBS 等）。

② 允许 DMZ 区内的应用服务器及工作站访问 Internet。

③ 禁止 DMZ 区的应用服务器访问内部网络。

④ 禁止外部网络非法用户访问内部网络等。

通常 DMZ 中服务器不应包含任何商业机密、资源代码或是私人信息。存放机密、私人信息的设备应部署在内部网络中。

由以上分析可知，要保证学校相关信息的机密性，就要避免外部网络的用户和内部网络中未经授权的用户直接访问存储学校机密数据的服务器、存储资源代码的 PC 和存储私人信息的 PC 等，因此需要将这些设备部署在校园网内部网络中以确保其安全。

对于邮件服务器、电子商务系统和应用网关等设备既要允许内、外网主机对其访问，又要保障它们的安全性。因此，这些设备需部署在防火墙的 DMZ 区域中。

2．案例参考答案

（1）标准化原则：所选择的设备必须基于国际标准或行业标准。因为只有基于标准的产品才有可能与其他厂商的产品互连互通。

可管理性原则：对于大型网络而言，这一点是至关重要的，它不仅关系到系统的性能指标，甚至关系到系统的可用性。主要考查网管系统对所选设备的监管、配置能力，以及设备可以提供的统计信息和故障检测手段，如骨干交换机必须具备端口镜像能力。这对于故障诊断，以及今后的网络规划具有特别重要的价值。

容错冗余性原则：除了在网络设计时要考虑冗余，骨干设备的容错冗余也是必须的。所谓容错，就是设备的某一模块出现故障时，是否会影响其他模块，乃至其他设备的正常工作；是否支持热插拔；是否支持备份设备的自动切换等。所谓冗余，就是配置的设备是否可以安装多个相同功能的模块，在工作正常的情况下实施负载分担，当其中一个出现问题时自动切换。

可扩展性原则：主干设备的选择应预留一定的扩展能力，而低端设备则够用即可。

保护原有投资原则：根据方案实际需要选型，即根据网络实际带宽性能需求、端口类型和端口密度等选型。尽量让旧设备降级纳入到新系统中，保护用户原有的投资。

（2）空（1）：Router1　　空（2）：Switch1　　空（3）：Switch2
　　空（4）：Switch3　　空（5）：Switch3

（3）空（6）：双千兆光纤链路　　空（7）：千兆光纤

空（8）：千兆双绞线　　　　　空（9）：百兆双绞线

（4）静态 IP 地址配置优点：每个用户拥有固定的 IP 地址，便于网络的管理以及资源的相互访问，无需配置专用的 IP 地址管理服务器。动态 IP 地址配置优点：可避免 IP 地址资源的浪费，增加了用户入网的灵活性。

空（1）：静态 IP 地址　　空（2）：静态 IP 地址　　空（3）：动态 IP 地址

（5）将 IP 地址与 MAC 地址进行绑定。

（6）区域 A 是 DMZ 区域。区域 A 中放置邮件服务器、应用网关、电子商务系统；内网中放置存储学校机密数据的服务器、存储资源代码的 PC 和存储私人信息的 PC。

DMZ 可以理解为一个不同于外网或内网的特殊网络区域。DMZ 内通常放置一些不含机密信息的公用服务器，如 Web、Mail 和 FTP 等。这样来自外网的访问者可以访问 DMZ 中的服务，但不可能接触到存放在内网中的公司机密或私人信息等。即使 DMZ 中服务器受到破坏，也不会对内网中的机密信息造成影响。

6.1.2　案例 2

阅读以下关于电子政务系统安全体系结构的叙述，回答问题 1～问题 4。

某城市计划建设电子政务系统，由于经费、政务应用成熟度和使用人员观念等多方面的原因，计划采用分阶段实施的策略来建设电子政务，最先建设急需和重要的部分。在安全建设方面，先投入一部分资金保障关键部门和关键信息的安全，之后在总结经验教训的基础上分两年逐步完善系统。因此，初步考虑使用防火墙、入侵检测、病毒扫描、安全扫描、日志审计、网页防篡改、私自拨号检测、PKI 技术和 FC SAN/IP SAN 等保障电子政务的安全。

在一次关于安全的方案讨论会上，张工认为由于政务网对安全性要求比较高，因此要建设防火墙、入侵检测、病毒扫描、安全扫描、日志审计、网页防篡改和私自拨号检测系统，这样就可以全面保护电子政务系统的安全。李工则认为张工的方案不够全面，还应该在张工提出的方案基础上，使用 PKI 技术进行认证、机密性、完整性和抗抵赖性保护，使用 FC SAN/IP SAN 提供数据安全和快速数据访问。

【问题 1】

请用 300 字以内文字，从网络安全方面，特别针对张工所列举的建设防火墙、入侵检测、安全扫描、日志审计系统进行分析，评论这些措施能够解决的问题和不能解决的问题。

【问题 2】

请用 300 字以内文字，主要从认证、机密性、完整性和抗抵赖性方面，论述李工的建议在安全上有哪些优点。

【问题 3】

对于复杂系统的设计与建设，在不同阶段都有很多非常重要的问题需要注意，既有

技术因素阻力，又有非技术因素阻力。请结合工程的实际情况，用200字以内文字，简要说明使用PKI还存在哪些重要的非技术因素方面的阻力。

【问题4】

请用300字以内文字，论述李工所提建议中的FC SAN和IP SAN的差别。

1．案例分析

（1）本问题主要是要求考生说明防火墙、入侵检测、病毒扫描、安全扫描和日志审计系统等常见的信息系统及网络安全防护技术的适用领域，以及其限制与约束。也就是要求考生能够正确地认识、选择与应用。

（2）PKI是CA安全认证体系的基础，为安全认证体系进行密钥管理提供了一个平台，它能够为所有网络应用透明地提供采用加密和数字签名等密码服务所必须的密钥和证书管理。PKI包括认证中心、证书库、密钥备份及恢复系统、证书作废处理系统及客户端证书处理系统等组成。

本小题要求考生深入了解PKI技术在认证、机密性、完整性和抗抵赖性方面的优点，并简要地做出描述。

（3）对于复杂系统的设计与建设，在不同阶段都有很多非常重要的问题需要注意，既有技术因素阻力，又有非技术因素阻力。而在网络安全的设计与实施方面，同样也会遇到非技术因素的阻力。本问题是在前一问题的基础上，要求考生能够对实施PKI时会遇到的非技术因素方面的阻力有清晰地认识，并简要地给出描述。

（4）SAN（Storage Area Network，存储区域网络）是一个由存储设备和系统部件构成的网络。所有的通信都在一个与应用网络隔离的单独的网络上完成，可以被用来集中和共享存储资源。SAN不但提供了对数据设备的高性能连接，提高了数据备份速度，还增加了对存储系统的冗余连接，提供了对高可用群集系统的支持。简单地说，SAN是关联存储设备和服务器的网络。它和以太网有类似的架构。以太网由服务器、以太网卡、以太网交换机及工作站组成。SAN则由服务器、HBA卡、交换机和存储装置所组成。

面对迅速增长的数据存储需求，大型企业和服务提供商开始选择SAN作为网络基础设施。SAN网络具有出色的可扩展性，理论上最多可以连接上万个设备。事实上，SAN比传统的存储架构具有更多优势。传统的服务器连接存储通常难于更新或集中管理。每台服务器必须关闭才能增加和配置新的存储。相比较而言，SAN不必宕机或中断与服务器的连接即可增加存储，还可以集中管理数据，从而降低总体拥有成本。利用协议技术，SAN可以有效地传输数据块。通过支持在存储和服务器之间传输海量数据块，SAN提供了数据备份的有效方式。因此，传统上用于数据备份的网络带宽可以节约下来用于其他应用。SAN可以分为FC SAN和IP SAN。本问题要求考生掌握FC SAN和IP SAN之间的差别。

2．案例参考答案

（1）防火墙是建立在内外网边界上的过滤封锁机制，它认为内网是可信的，外网是

不可信的。它能够防止外网未经授权地访问内网，能够防止外网对内网的攻击，也能防止内网未经授权地访问外网。但是，根据统计，绝大多数的网络攻击来自于内网，而防火墙不能阻止内网的攻击，因此，仅使用防火墙不能有效地防止网络攻击。

入侵检测系统的目的在于提供实时的入侵检测及采取相应的防护手段，它的能力要点在于能够对付来自内部的攻击。如果能够实现入侵检测系统和其他安全系统，例如防火墙的联动，则能够更加有效地防止网络攻击。但是，目前的入侵检测系统对已知的攻击有较好的检测，对未知的攻击检测能力较弱，而且存在误报率太高的缺点。

安全扫描：主要用于发现安全漏洞。

日志审计有助于追查责任，定位故障，系统恢复。

防火墙、入侵检测、安全扫描、日志审计有各自的应用目的和优点，但不能全面解决网络安全问题。

（2）防火墙、入侵检测、病毒扫描、安全扫描、日志审计、网页防篡改、私自拨号检测系统都不能解决政务网中的认证、机密性、完整性和抗抵赖性问题。

身份认证能够解决通信或数据访问中对对方身份的认可，便于访问控制，授权管理。电子政务还有其他的安全需求，机密性防止信息在传输、存储过程中被泄露。

完整性防止对数据进行未授权的创建、修改或破坏，使数据一致性受到损坏。

抗抵赖性有助于责任追查。

（3）对于复杂系统的设计与建设，有许多非常重要的问题。有关使用 PKI 的非技术因素阻力如下。

① 对所有系统的有关设计、开发、使用、维护和管理等人员进行必要的安全教育，使大家认识到信息安全的重要性。

② 在系统的设计、建设、运行阶段都要投入大量的资金，需要充分咨询相关领域专家。

③ 在系统的设计、建设、运行阶段，需要对不同的设计、开发、使用、管理和维护等人员进行针对性的培训。

④ 相关法律与法规制度的建立、执行与监督。

（4）FC SAN 和 IP SAN 的主要区别如下。

FC SAN 使用专用光纤通道设备，IP SAN 使用通用的 IP 网络及设备，因此 FC SAN 与 IP SAN 相比传输速度高，但价格比 IP SAN 昂贵。

从应用上来说，相对于 IP SAN，FC SAN 可以承接更多的并发访问用户数。当并发访问存储的用户数不多时，FC SAN 对比 IP SAN 二者性能相差无几。但一旦外接用户数呈大规模增长趋势时，FC SAN 就显示出其在稳定、安全以及高性能传输率等方面的优势。

FC SAN 比 IP SAN 的稳定性高，FC SAN 由于使用高效的光纤通道协议，因此大部分功能都是基于硬件来实现的，如后端存储子系统的存储虚拟通过带有高性能处理器的

专用 RAID 控制器来实现，中间的数据交换层通过专用的高性能 ASIC 来进行基于硬件级的交换处理，在主机端通过带有 ASIC 芯片的专用 HBA 来进行数据信息的处理。因此在大量减少主机处理开销的同时，也提高了整个 FC SAN 的稳定性。

在安全性方面，FC SAN 是服务器后端的专用局域网络，安全性比较高。基于 iSCSI 标准的 IP SAN 提供了 initiator 与目标端两方面的身份验证（使用 CHAP、SRP、Kerberos 和 SPKM），能够阻止未经授权的访问，只允许那些可信赖的节点进行访问。另外，IPSec 协议确保了数据私密性。因此，两者的安全性都较好。

由于 IP 技术的普及和发展，利用 iSCSI 技术搭建的 IP SAN 可以随着网络延伸至全球任意一个角落，从根本上解决了信息孤岛的问题。甚至可以通过 IP SAN 来连接各个 FC SAN 的孤岛，因此 IP SAN 比 FC SAN 具有更好的伸展性。

6.2 网络优化案例

某企业网络的拓扑结构如图 6-2 所示，阅读以下关于该企业网络结构的描述，然后回答问题 1 至问题 4。

图 6-2 某企业网络拓扑结构图

（1）某企业网络由总公司和分公司组成，其中分公司的网络自治系统 2（AS 2）采

用 OSPF 路由协议，总公司的网络自治系统 1（AS 1）采用 RIPv2 路由协议。

（2）该企业网络有两个出口，一个出口通过 Router1 的 S0 端口连接 ISP1，另一个出口通过 Router1 的 S1 端口连接 ISP2。

（3）路由器 Router1 的 Fa0/0 端口连接 LAN3，该端口的 IP 地址为 192.168.3.1/24。Router1 的 Fa0/0、Fa0/1、Fa0/2 端口启用了 RIPv2 协议。Router1 的 Fa0/3 端口启用了 OSPF 协议。

（4）路由器 Router2 的 Fa0/0 端口连接 LAN 1，其 IP 地址为 192.168.1.1/24，在该端口启用了 RIPv2 协议。

（5）路由器 Router5 的 Fa0/1 端口连接 LAN 2（192.168.2.0/24），该端口的 IP 地址为 192.168.2.1/24。

【问题 1】

与 Router2 连接的局域网 LAN 1 是一个末节网络，而且已接近饱和，为了减少流量，需要过滤进入 LAN 1 的路由更新，可以采用什么方法实现？请写出配置过程。

【问题 2】

LAN 2 中的计算机不需要访问 LAN 3 中的计算机，为了进一步控制流量，网络管理员决定通过访问控制列表阻止 192.168.2.0/24 网络中的主机访问 192.168.3.0/24 网络，请问应将访问控制列表设置在哪台路由器上？如何配置？

【问题 3】

如果希望采用策略路由将来自 192.168.3.0/24 网络去往 Internet 的数据流转发到 ISP1，将来自 192.168.2.0/24 网络去往 Internet 的数据流转发到 ISP2，应如何配置？

【问题 4】

要求自治系统 1 中的路由器 Router2 能学习到自治系统 2（OSPF 网络）中的路由信息，同时 Router3 也能学习到自治系统 1 中的路由信息，应采用什么方法？请写出配置过程。

1．案例分析

网络管理员可以通过设置路由器何时交换路由更新以及路由更新中应包含哪些信息来优化网络中的路由。本案例主要考查路由优化方面的相关知识，包括路由更新控制、基于策略的路由和路由重发布等。

（1）问题 1 需要过滤进入 LAN 1 的路由更新，则可以将连接 LAN 1 的 Fa0/0 端口配置为被动接口。被动接口只接收路由更新但不发送路由更新。passive-interface 命令可以用于所有 IP 内部网关协议（包括 RIP、IGRP、EIGRP、OSPF 和 IS-IS），该命令的语法如下：

```
Router(config-router)# passive-interface type number
```

（2）为了过滤不必要的通信流量，可以通过配置访问列表来实现。问题 2 主要考查

配置访问控制列表的原则和方法。访问控制列表是应用于路由器接口的指令列表，用于指定哪些数据包可以接收并转发，哪些数据包需要拒绝，ACL 可以限制网络流量、提高网络性能。ACL 的工作原理是读取数据包中第三层及第四层头部中的源 IP、目的 IP 和目的端口等信息，然后根据预先定义好的规则对包进行过滤。

访问控制列表的种类包括标准访问控制列表和扩展访问控制列表。其中，标准访问控制列表根据数据包的源 IP 地址决定转发或丢弃数据包，其常用的访问控制列表号从 1 到 99。扩展访问控制列表基于源 IP、目的 IP、传输层协议和应用服务端口号进行过滤，使用扩展 ACL 可实现更加精确的流量控制，其常用的访问控制列表号从 100 到 199。

ACL 通过过滤数据包并且丢弃不希望抵达目的地的数据包来控制通信流量。然而能否有效地减少不必要的通信流量，还要取决于网络管理员把 ACL 部署在哪个地方。其部署原则是：标准 ACL 要尽量靠近目的端，扩展 ACL 则要尽量靠近源端。因此，本小题应在路由器 Router5 上配置扩展访问控制列表。

（3）本小题要求考生掌握策略路由的原理及其配置方法。通过策略路由，路由器可以按照事先设置好的规则根据数据包的目的 IP 或源 IP 来选择路由。尽管策略路由可以用于在 AS 中控制数据流，但它通常用于控制 AS 间的路由。

route-map 命令用于配置策略路由，其语法如下：

```
Router(config)# route-map map-tag {permit|deny} [sequence-number]
Router(config-map-router)#
```

参数 map-tag 是该路由图的标识符，可以将其设置为容易理解的字符串，例如 ISP2。route-map 命令将把路由器的模式改变为路由图配置模式（config-map-router），在该模式下，可以为路由图配置条件。每个 route-map 命令中都有一组 set 和 match 命令。match 命令用于指定匹配准则，set 命令用于设置满足匹配条件时要采取的动作。

路由图的运行机理和访问控制列表相似，都是逐行进行检查，遇到匹配就立即进行处理。

（4）本小题要求考生掌握路由重发布相关基本知识及配置方法。为了在互联网络中高效地支持多种路由选择协议，必须在这些不同的路由协议之间共享路由信息。例如，从 RIP 路由进程所学习到的路由可能需要被注入到 IGRP 路由进程中去。在路由选择协议之间交换路由信息的过程称为路由重发布。这种重发布可以是单向的或双向的，单向是指一种路由协议从另一种路由协议那里接收路由，双向是指两种路由选择协议互相接收对方的路由。执行路由重发布的路由器称为边界路由器，因为它处于两个或者多个自治系统或路由域的边界上。

根据本小题的要求，应该在路由器 Router1 上配置双向路由重发布。

2．案例参考答案

（1）为了阻止路由更新进入 LAN 1，可以将路由器 Router2 的 Fa0/0 端口配置为被

动接口。

```
Router2(config)# router rip
Router2(config-router)# passive-interface fa0/0
```

（2）应将访问控制列表设置在路由器 Router5 上，配置方法如下：

```
Router5(config)# access-list 101 deny ip 192.168.2.0 0.0.0.255 192.168.3.0
0.0.0.255
Router5(config)# access-list 101 permit ip any any
Router5(config)# int fa0/1
Router5(config-if)# ip access-group 101 in
```

（3）可以在路由器 Router1 上配置策略路由，其配置方法如下：

```
Router1(config)# access-list 1 permit 192.168.3.0 0.0.0.255
Router1(config)# access-list 2 permit 192.168.2.0 0.0.0.255
Router1(config)# route-map ISP1 permit 10
Router1(config-route-map)# match ip address 1
Router1(config-route-map)# set interface serial 0
Router1(config-route-map)# exit
Router1(config)# route-map ISP2 permit 20
Router1(config-route-map)# match ip address 2
Router1(config-route-map)# set interface serial 1
```

然后将每个路由图应用到路由器 Router1 的适当接口上，这里的适当接口是指那些数据流进入路由器的接口。

```
Router1(config)# interface fa0/0
Router1(config-if)# ip policy route-map ISP1
Router1(config-if)# interface fa0/1
Router1(config-if)# ip policy route-map ISP2
Router1(config-if)# interface fa0/2
Router1(config-if)# ip policy route-map ISP2
```

（4）可以在两个自治系统的边界路由器 Router1 上设置路由重发布，配置过程如下。配置 OSPF 协议和路由重发布命令：

```
Router1(config)# router ospf 101
Router1(config-router)# redistribute rip subnets
Router1(config-router)# network X.X.X.X wildcard area 0
```

配置 RIP 协议和路由重发布：

```
Router1(config)# router rip
```

```
Router1(config-router)# network X.X.X.X //配置多条 network 命令
Router1(config-router)# passive-interface fa0/3
Router1(config-router)# redistribute ospf 101 match internal external 1
external 2
Router1(config-router)# default-metric 10
```

6.3 网络配置案例

6.3.1 案例 1

阅读以下关于某网络结构的描述，然后回答问题 1 至问题 5。

网络拓扑结构如图 6-3 所示，交换机均为 Cisco Catalyst 2960，路由器均为 Cisco 2621，路由器各接口 IP 参数如表 6-2 所示。

表 6-2 设备及接口信息表

路 由 器	接 口	IP 参数
Router1	Fa0/0	202.114.66.5/30
	Fa0/1	192.168.1.254/24
Router2	Fa0/0	?
	S1/1 （DCE 端）	?
Router3	S1/1	202.114.66.9/30
	Fa0/0	202.114.64.1/24
	Fa0/1	202.114.67.1/24

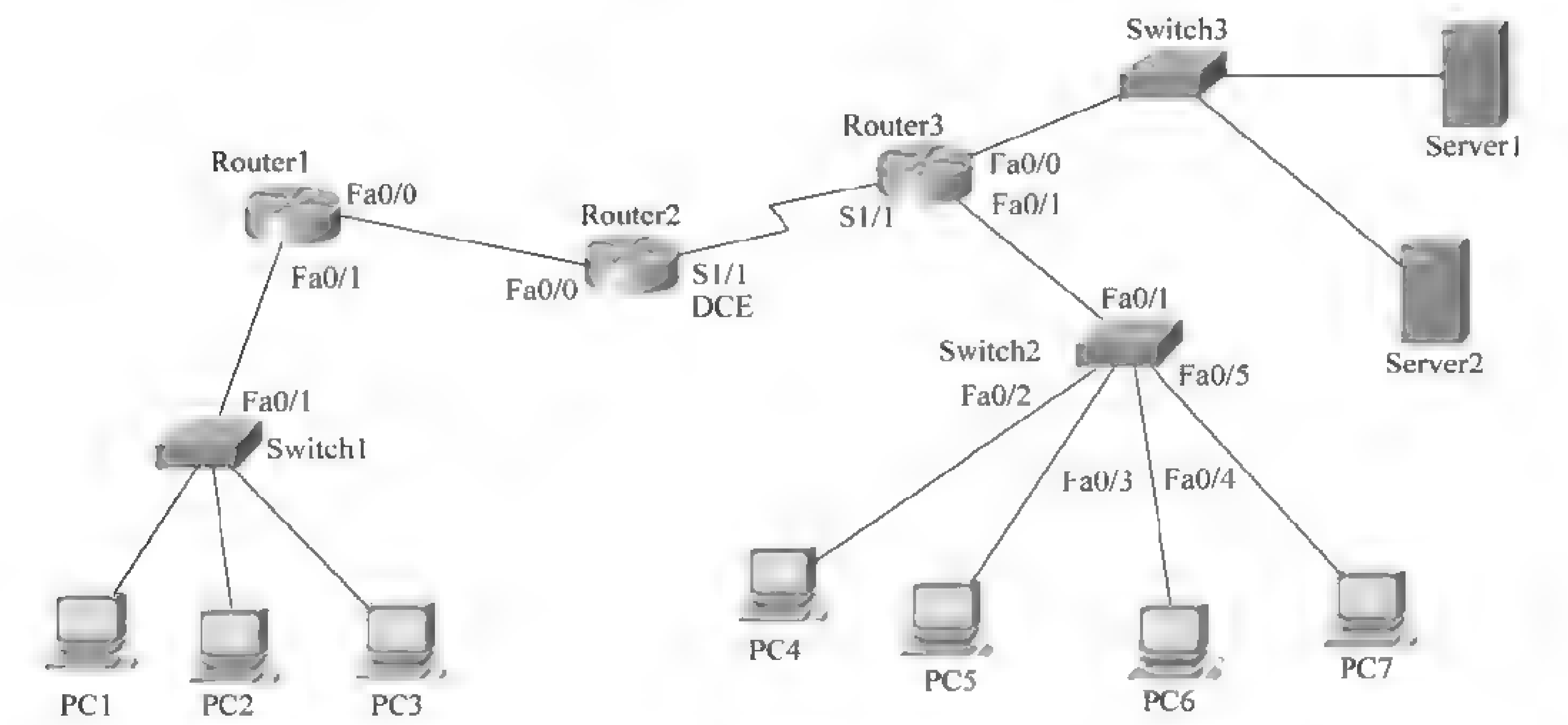


图 6-3 网络拓扑结构

【问题 1】

为路由器 Router2 规划 IP 地址，并说明选择所规划 IP 地址及子网掩码的理由，为 Fa0/0 和 S1/1 接口配置 IP 地址并启用接口。

【问题 2】

因 IP 地址紧张，路由器 Router1 Fa0/1 接口所连接的局域网分配内部 IP 地址 192.168.1.X/24，现要求在 Router1 中配置网络地址转换（NAT），外部地址为 Fa0/0 接口的地址 202.114.66.5/30。并请简要说明路由器 Router1 实施网络地址转换的过程。

【问题 3】

在路由器 Router3 中配置 DHCP 服务，为 Fa0/1 接口连接的局域网动态分配 IP 地址，域名服务器的 IP 为 202.114.64.2，地址租期为 30 天，该局域网中有一台服务器已配置静态 IP 202.114.67.8/24，请写出配置过程。

【问题 4】

路由器 Router2 和 Router3 之间的链路采用 PPP 协议封装，要求采用安全的认证方式。请写出配置过程并简要注释。

【问题 5】

假如该网络采用 RIP 路由协议，请写出路由器 Router3 中的配置过程。

1．案例分析

掌握网络设备的配置方法是网络规划师的基本技能之一，本案例主要是考查以下知识点。

（1）对子网掩码和变长子网掩码的理解。VLSM（Variable Length Subnet Mask，变长子网掩码）是一种产生不同大小子网的网络分配机制，指一个网络可以配置不同的掩码。提出变长度子网掩码的想法就是在每个子网保留足够主机数的同时，把一个子网进一步分成多个小子网以便更有效地节省 IP 地址。如果没有 VLSM，在一个网络中只能采用同样的子网掩码，这样每个子网中具有相同的主机数，缺乏灵活性。

VLSM 技术对高效分配 IP 地址（较少浪费）以及减小路由表都起到非常重要的作用，但是需要注意的是，使用 VLSM 时，所采用的路由协议必须能够支持它，这些路由协议包括 RIP2、OSPF、EIGRP 和 BGP。换言之，无类路由选择网络中可以使用 VLSM，而在有类路由选择网络中不能使用 VLSM。

（2）掌握路由器接口的配置方法。

```
Router(config)# interface type slot/port    //进入接口配置模式
Router(config-if)# ip address IP_address subnet_mask
                                            //设置接口的 IP 地址和子网掩码
Router(config-if)# clock rate 64000         //配置接口时钟，这个命令用于 DCE 设备
Router(config-if)# no shutdown              //开启一个接口
Router(config-if)# description string       //为接口设置描述字符串，在大型网络中
```

```
                                        //方便管理员掌握该接口连接的设备或位置信息
Router(config-if)# bandwidth rate in Kbps   //改变该接口的带宽值
```

（3）掌握 NAT 的工作原理及配置方法。

IP 地址耗尽促成了 CIDR 的开发，但 CIDR 开发的主要目的是为了有效使用现有 Internet 地址，而同时根据 RFC 1631（The IP Network Address Translator）开发的 NAT 技术却可以让多台主机使用相同的 IP 地址连接到 Internet，用来减少注册 IP 地址的使用。

NAT 技术使得一个私有网络可以通过 Internet 注册 IP 连接到外部世界，位于 inside 网络和 outside 网络间的 NAT 路由器在向外部发送数据包之前，负责把内部 IP 翻译成外部合法地址。NAT 的翻译可以采取静态翻译（Static Translation）和动态翻译（Dynamic Translation）两种方法。静态翻译将内部地址和外部地址一一对应，动态翻译则是根据需要将内部地址动态转换为地址池（pool）中的外部地址。通过改变向外发送数据包的源端口可以将多个内部 IP 地址映射到同一个外部地址，这就是 PAT 技术（Port Address Translator）。

NAT 配置的常用命令如下。

- ip nat {inside|outside}：接口配置命令，至少在一个内部和一个外部接口上启用 NAT。
- ip nat inside source static *local-ip global-ip*：全局配置命令，在对内部局部地址使用静态地址转换时，用该命令进行地址定义。
- access-list *access-list-number* {permit|deny} *local-ip-address*：使用该命令为内部网络定义一个标准的 IP 访问控制列表。
- ip nat pool *pool-name start-ip end-ip netmask netmask* [type rotary]：使用该命令为内部网络定义一个 NAT 地址池。
- ip nat inside source list *access-list-number* pool *pool-name* [overload]：使用该命令定义访问控制列表与 NAT 内部全局地址池之间的映射。
- ip nat outside source list *access-list-number* pool *pool-name* [overload]：使用该命令定义访问控制列表与 NAT 外部局部地址池之间的映射。
- ip nat inside destination list *access-list-number* pool *pool-name*：使用该命令定义访问控制列表与终端 NAT 地址池之间的映射。
- show ip nat translations：显示当前存在的 NAT 转换信息。
- show ip nat statistics：查看 NAT 的统计信息。
- show ip nat translations verbose：显示当前存在的 NAT 转换的详细信息。
- debug ip nat：跟踪 NAT 操作，显示出每个被转换的数据包。
- clear ip nat translations *：删除 NAT 映射表中的所有内容。

（4）掌握 DHCP 工作原理，并熟悉如何在路由器中配置 DHCP 服务。

DHCP 服务器能够自动为网络中的计算机提供 IP 地址等网络参数，考生不仅要掌握

Windows/Linux 中的 DHCP 服务配置方法，也要掌握在路由器中如何配置 DHCP 服务。

```
Router(config)# ip dhcp pool pool-name          //配置地址池
Router(dhcp-config)# network ip network subnet mask //设置动态分配的地
                                                      //址段
Router(dhcp-config)# domain-name test.com       //为客户机配置域后缀
Router(dhcp-config)# dns-server IP address      //为客户机配置 DNS 服务器
Router(dhcp-config)# default-router IP_address  //为客户机配置网关 IP 地址
Router(dhcp-config)# lease n                    //设置地址租用期为 n 天
```

在整个网络中，有些 IP 地址需要静态地指定给一些特定的设备，如路由器的端口、DNS 服务器和 WWW 服务器等。显然，这些静态 IP 地址是不能用于动态分配的，这就需要将它们排除掉。其配置命令如下：

```
Router(dhcp-config)# ip dhcp excluded-address start-ip end-ip
```

（5）掌握 PPP 协议和 RIP 协议的原理及配置方法。

PPP 协议中提供了一整套方案来解决链路建立、维护、拆除、上层协议协商和认证等问题。PPP 协议包含链路控制协议（Link Control Protocol，LCP）和网络控制协议（Network Control Protocol，NCP）。PPP 支持用户认证，最常用的认证方式包括口令验证协议（Password Authentication Protocol，PAP）和 CHAP 协议（Challenge-Handshake Authentication Protocol）。

RIP（Routing Information Protocol）是应用较早、使用较普遍的内部网关协议（Interior Gateway Protocol，IGP），适用于小型网络，是典型的距离向量协议。协议文档见 RFC 1058 和 RFC1723。

```
Router(config)# router rip                   //指定使用 RIP 协议
Router(config-router)# version {1|2}         //指定 RIP 版本
Router(config-router)# network ip_network    //设置允许路由的网络
```

2．案例参考答案

（1）根据链路对端的 IP 地址及子网掩码，可计算出 Router2 Fa0/0 端口的 IP 地址为 202.114.66.6/30，S1/1 端口的 IP 地址为 202.114.66.10/30。

```
Router2(config)# interface fa0/0
Router(config-if)#ip address 202.114.66.6 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#interface serial1/1
Router(config-if)#ip addr 202.114.66.10 255.255.255.252
Router(config-if)#clock rate 64000
Router(config if)#no shutdown
```

（2）Router1(config)# interface fa0/1

```
Router1(config-if)#ip address 192.168.1.254 255.255.255.0
Router1(config-if)#ip nat inside
Router1(config-if)#interface fa0/0
Router1(config-if)#ip address 202.114.66.5 255.255.255.252
Router1(config-if)#ip nat outside
Router1(config)#ip nat inside source list 1 interface FastEthernet0/0
overload
Router1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

当内网计算机发出的数据包经过路由器 Router1 时，路由器 Router1 替换数据包中的源 IP 和源 port，并建立映射表。当外网计算机发来的响应数据包经过路由器 Router1 时，路由器根据 NAT 映射表替换目标 IP 和目标 port，然后转发到内网。

（3）Router3(config)# ip dhcp pool lan67

```
Router3(dhcp-config)# network 202.114.67.0 255.255.255.0
Router3(dhcp-config)# ip dhcp excluded-address 202.114.67.1
Router3(dhcp-config)# ip dhcp excluded-address 202.114.67.8
Router3(dhcp-config)# dns-server 202.114.64.2
outer3(dhcp-config)# default-router 202.114.67.1
outer3(dhcp-config)# lease 30
```

（4）Router2(config)#hostname router2

```
outer2(config)#username router3 password cisco  //配置用于认证的用户名及
                                                 //密码
outer2(config)#interface serial1/1
outer2(config-if)#encapsulation ppp              //设置封装 PPP 协议
outer2(config-if)#ppp authentication chap        //设置 PPP 认证方式为 CHAP

outer3(config)#hostname router3                  //设置路由器主机名
outer3(config)#username router2 password cisco  //配置用于认证的用户名及
                                                 //密码
    outer3(config)#interface serial1/1
    outer3(config-if)#encapsulation ppp          //设置封装 PPP 协议
    outer3(config-if)#ppp authentication chap    //设置 PPP 认证方式为 CHAP
```

（5）Router3(config)#router rip

```
Router3(config-router)#version 2
Router3(config-router)#network 202.114.66.0
Router3(config router)#network 202.114.64.0
```

```
Router3(config-router)#network 202.114.67.0
Router3(config-router)#no auto-summary
```

6.3.2　案例 2

VPN 是一种能够通过共享的网络基础设施如因特网，来提供安全、可靠连接的服务。站点到站点 VPN 可以用于连接公司之间的站点，过去，公司之间的连接通常使用租用 X.25/DDN 专线或帧中继，但现在可通过 VPN 代替以节省成本。图 6-4 是某企业的总公司和子公司通过支持 VPN 的防火墙构建的站点到站点 VPN。

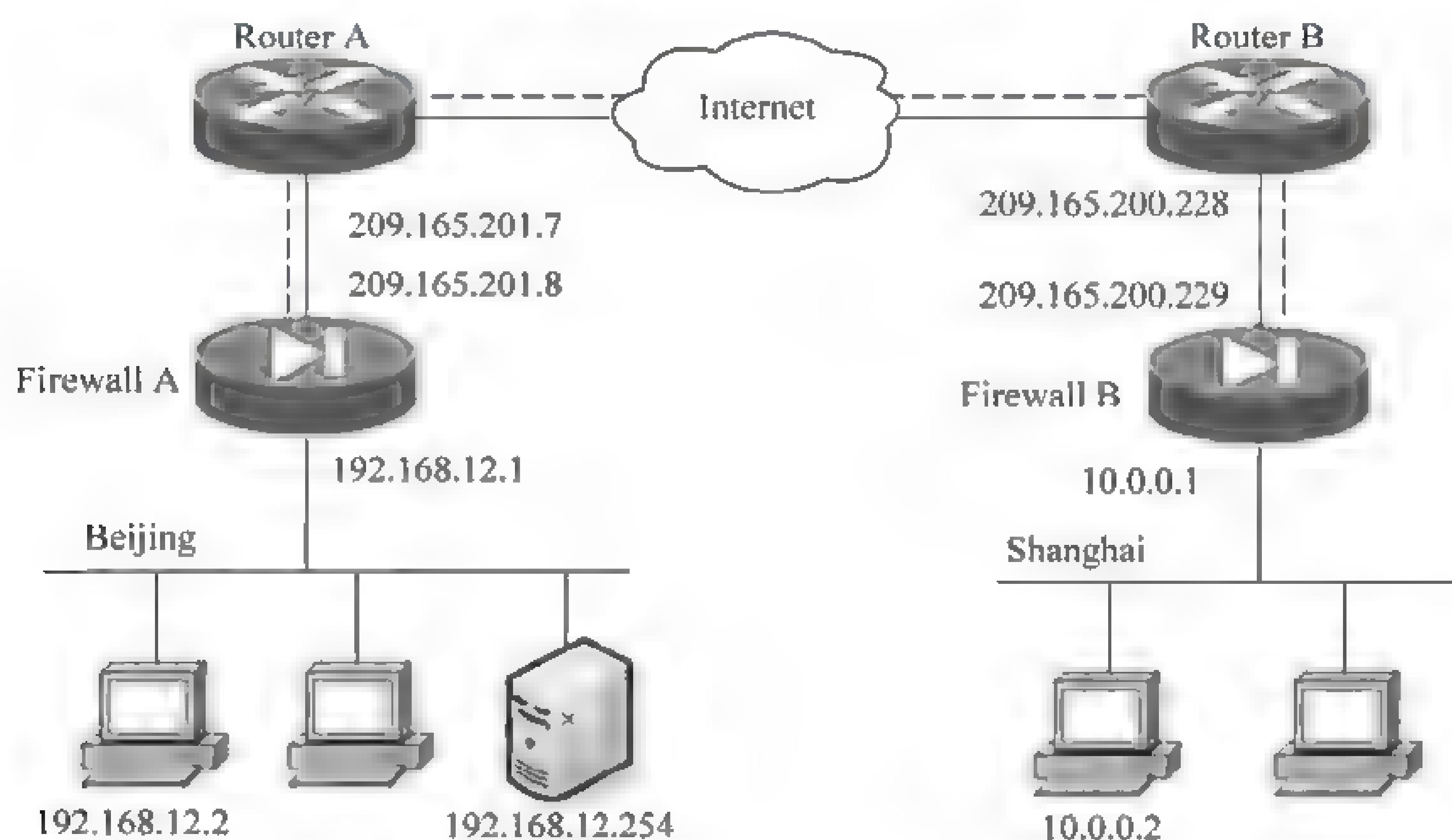


图 6-4　站点到站点 VPN

【问题 1】

Firewall-A 的部分配置如下，请对配置命令给出注释。

```
hostname Beijing
access-list 90 permit ip 192.168.12.0 255.255.255.0 10.0.0.0 255.0.0.0
global (outside) 1 209.165.202.129-209.165.202.159
global (outside) 1 209.165.202.160
nat 0 access-list 90
nat (inside) 1 0 0
isakmp enable outside
isakmp policy 9 authentication pre-share
isakmp policy 9 encrypt des
Isakmp policy 9 hash sha
Isakmp policy 10 lifetime 86400
```

```
crypto isakmp key cisco1234 address 209.165.200.229
crypto ipsec transform-set strong esp-des esp-sha-hmac
crypto map Shanghai 20 ipsec-isakmp
crypto map Shanghai 20 match address 90
crypto map Shanghai 20 set transform-set strong
crypto map Shanghai 20 set peer 209.165.200.229
crypto map Shanghai interface outside
sysopt connection permit-ipsec
route outside 0.0.0.0 0.0.0.0 209.165.201.7 1
```

【问题 2】

Firewall 可以使用 AAA 对进站连接和出站连接进行控制，现在要求当图中 192.168.12.0/24 网段中的用户访问 Internet 时，Firewall 会对用户进行验证，只有当用户输入正确的用户名和密码后，Firewall 才会允许用户的访问，请写出配置 AAA 的相关命令。假定网络中有一台 Radius 服务器，其 IP 地址为 192.168.12.254。

【问题 3】

请简单叙述 IPSec 是如何工作的。

1. 案例分析

本案例主要是考查以下知识点。

（1）深入了解 VPN 相关知识，并掌握 VPN 的配置方法。

通过对网络数据的封包和加密传输，在公用网上传输私有数据、达到私有网络的安全级别，从而利用公用网构筑企业网络，这就是虚拟私有网络（Virtal Private Network，VPN）。如果接入方式为拨号方式，则称之为 VPDN。VPN 通过公众 IP 网络建立了私有数据传输通道，将远程的分支办公室、商业伙伴和移动办公人员等连接起来。减轻了企业的远程访问费用负担，节省电话费用开支，并且提供了安全的端到端的数据通信。

目前，VPN 主要采用 4 项技术来保证安全，这 4 项技术分别是隧道技术（Tunneling）、加解密技术（Encryption & Decryption）、密钥管理技术（Key Management）和使用者与设备身份认证技术（Authentication）。

隧道技术是 VPN 的基本技术，类似于点对点连接技术，它在公用网建立一条数据通道（隧道），让数据包通过这条隧道传输。隧道是由隧道协议形成的，分为第二、三层隧道协议。第二层隧道协议是先把各种网络协议封装到 PPP 中，再把整个数据包装入隧道协议中。这种双层封装方法形成的数据包靠第二层协议进行传输。第三层隧道协议是把各种网络协议直接装入隧道协议中，形成的数据包依靠第三层协议进行传输。第二层隧道协议有 L2F、PPTP 和 L2TP 等，第三层隧道协议有 IPSec 等。本案例主要考查 IPSec VPN 的相关知识。

（2）理解 AAA 协议。

访问控制是用来控制接入网络或访问网络资源的用户，并限制他们可使用的服务种

类。AAA（Authentication、Authorization、Accounting，身份认证、授权、审计）协议所提供的功能是为了提高网络安全性。

- Authentication：主要功能是提供用户凭证以获得对一个系统访问的权利。主要验证用户有没有接入到网络中的凭证，如果没有，则拒绝接入其网络。
- Authorization：用户接入到网络中，控制用户使用网络的权利，例如用户只能查看网络设备的状态，不能对其进行修改等。
- Accounting：主要记录用户登录网络中所做的活动，详细记录用户何时、何处做了什么。

AAA 的体系结构包括如下三部分。

- AAA 的服务器：安装了 ACS 软件的服务器。
- AAA 的客户端：支持 AAA 服务的各种网络设备。
- AAA 协议：负责在服务器和客户端之间进行认证信息交互，常用 TACACS+、RADIUS 和 Kerberos 三种协议。

（3）在了解 IPSec 工作原理的基础上掌握其工作过程。

IPSec（Internet Protocol Security，Intenet 安全协议）是 IETF 提供 Internet 安全通信的一系列规范，它提供私有信息通过公用网的安全保障。IPSec 适用于目前的 IPv4 和下一代 IPv6。IPSec 将几种安全技术结合形成一个完整的安全体系，它包括安全协议部分和密钥协商部分。

① 安全关联和安全策略：安全关联（Security Association，SA）是构成 IPSec 的基础，是两个通信实体经协商建立起来的一种协定，它们决定了用来保护数据包安全的安全协议（AH 协议或者 ESP 协议）、转码方式、密钥及密钥的有效存在时间等。

② IPSec 协议的运行模式：IPSec 协议的运行模式有两种，IPSec 隧道模式及 IPSec 传输模式。隧道模式的特点是数据包最终目的地不是安全终点。通常情况下，只要 IPSec 双方有一方是安全网关或路由器，就必须使用隧道模式。传输模式下，IPSec 主要对上层协议即 IP 包的载荷进行封装保护，传输模式常用于两台主机之间的安全通信。

③ AH（Authentication Header，认证头）协议：设计 AH 认证协议的目的是用来增加 IP 数据报的安全性。AH 协议提供无连接的完整性、数据源认证和抗重放保护服务，但是 AH 不提供任何保密性服务。

④ ESP（Encapsulate Security Payload，封装安全载荷）协议：用于提高 Internet 协议的安全性。它可为 IP 提供机密性、数据源验证、抗重放以及数据完整性等安全服务。

⑤ Internet 密钥交换协议（IKE）：是 IPSec 默认的安全密钥协商方法。IKE 通过一系列报文交换为两个实体（如网络终端或网关）进行安全通信派生会话密钥。IKE 建立在 Internet 安全关联和密钥管理协议（ISAKMP）定义的一个框架之上。IKE 是 IPSec 目前正式确定的密钥交换协议，IKE 为 IPSec 的 AH 和 ESP 协议提供密钥交换管理。

2．案例参考答案

（1）关键配置命令的注释如下：

```
hostname Beijing        //设置主机名
access-list 90 permit ip 192.168.12.0 255.255.255.0 10.0.0.0 255.0.0.0
                        //该访问列表定义总公司去往子公司间的流量
global (outside) 1 209.165.202.129-209.165.202.159 //定义外部地址池用于
                                                   //NAT 或 PAT
global (outside) 1 209.165.202.160
nat 0 access-list 90    //将访问列表 90 排除在 NAT 之外
nat (inside) 1 0 0      //对其他的所有流量进行 NAT 转换
isakmp enable outside   //在 outside 接口上启动 IKE
isakmp policy 9 authentication pre-share    //定义 IKE 策略，优先级为 9，认证
                                            //方式采用预共享密钥方式
isakmp policy 9 encrypt des     //配置加密方式为 des（用于数据加密）
Isakmp policy 9 hash sha        //配置 hash 算法为 sha（用于鉴别数据包）
Isakmp policy 10 lifetime 86400 //指定 IKE SA 的生存时间
crypto isakmp key cisco1234 address 209.165.200.229     //配置预共享密钥
                                                        //并和对端关联
crypto ipsec transform-set strong esp-des esp-sha-hmac
//配置交换集，名称为 strong，交换集被设计用于为数据流制定一个特定的安全策略
crypto map Shanghai 20 ipsec-isakmp     //配置加密图
crypto map Shanghai 20 match address 90 //配置上面的访问列表 90 为加密数据流
crypto map Shanghai 20 set transform-set strong //指定该 IPSec 加密图使用的
                                                //交换集为 strong
crypto map Shanghai 20 set peer 209.165.200.229 //配置 VPN 对等体
crypto map Shanghai interface outside   //将加密图 Shanghai 应用到 outside
                                        //接口
sysopt connection permit-ipsec          //配置信任 IPSec 流量
route outside 0.0.0.0 0.0.0.0 209.165.201.7 1   //配置默认路由
```

（2）配置 AAA 服务器参数：

```
firewall(config)# aaa-server test protocol radius
firewall(config)# aaa-server test (inside) host 192.168.12.254 cisco
```

配置 AAA 认证：

```
firewall(config)# access-list access-internet extended permit ip any any
firewall(config)# aaa authentication match access-internet inside test
```

（3）IPSec 的目标是用必要的安全服务保护有用的数据。IPSec 的操作可以分成 5 个

主要的步骤。

① 定义感兴趣的数据流。当用户发送的业务流需要保护时，将其定义为感兴趣的数据流。VPN 设备会将这种数据流通过 IPSec 隧道传送。对于 IPSec 保护的每个数据包，系统管理员必须指定数据包所用的安全服务。安全策略数据库将指定数据流所使用的 IPSec 协议、模式和算法。

② IKE 阶段 1。在对等体之间，协商并确定了一套最基本的安全服务，这一套基本的服务将保护对等体之间发生的后续通信服务。IKE 阶段 1 的目的是协商 IKE 策略集、认证对等体并在对等体之间建立安全的信道。

③ IKE 阶段 2。IKE 协商 IPSec 安全关联参数，并在对等体中建立相匹配的 IPSec 安全关联。这些安全参数用于保护端点之间交换的数据和消息。该阶段主要执行以下功能。

- 协商 IPSec 安全性参数和 IPSec 转换集。
- 建立 IPSec 的 SA。
- 定期重协商 IPSec 的 SA，以确保安全性。
- 可以执行额外的 DH 交换。

④ 数据传输。基于保存在安全关联数据库中的 IPSec 参数和密钥，在 IPSec 对等体间传送数据。

⑤ IPSec 隧道终止。可以通过删除或超时的方式将 IPSec SA 终止。超过规定的秒数或当一定数量的字节通过隧道后，SA 就会超时。SA 终止时，密钥也会被丢弃。如果数据流需要后续的 IPSec SA，则 IKE 将执行新的协商。协商成功后将会产生新的 SA 和新的密钥。

6.4　网络故障分析与处理案例

阅读以下描述，然后回答问题 1 至问题 4。

某企业局域网拓扑结构如图 6-5 所示，三台交换机互相通过快速以太网端口连接。在交换机 Switch2 上创建有基于端口的 VLAN，其中 Fa0/3 属于 VLAN 3，Fa0/4 属于 VLAN5。交换机 Switch3 上也创建有基于端口的 VLAN，其中 Fa0/3 属于 VLAN 3，Fa0/4 属于 VLAN5。4 台 PC 的 IP 地址如下。

PC1：192.168.1.11/24　　PC2：192.168.1.12/24

PC3：192.168.1.13/24　　PC4：192.168.1.14/24

【问题 1】

管理员发现交换机 Switch2 的 Fa0/1 端口指示灯显示异常，但用 show interface fa0/1 命令查看该端口信息如下，试问 Fa0/1 端口处于什么状态？为什么？

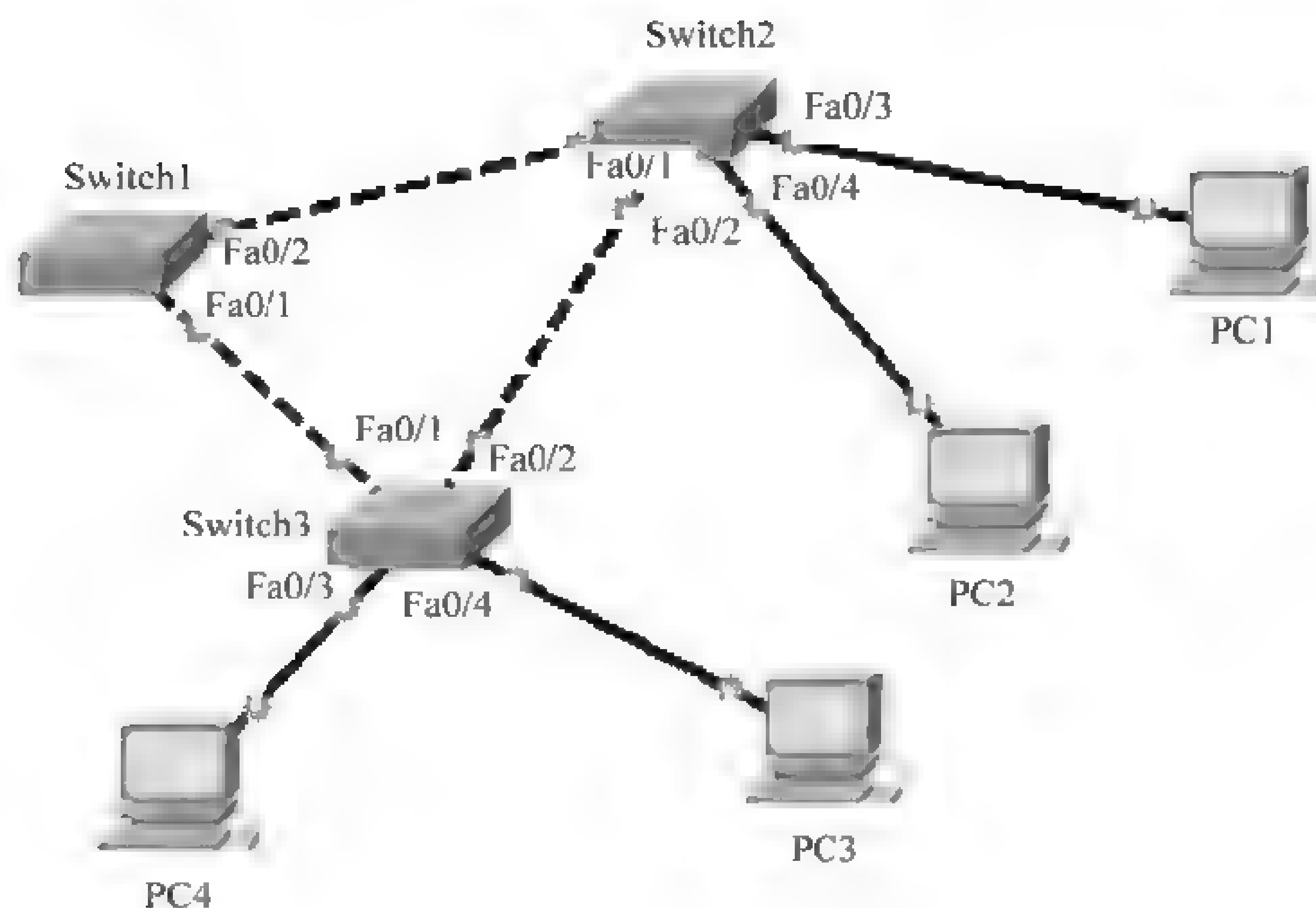


图 6-5 某企业局域网拓扑结构

```
Switch#show int  fa0/1
FastEthernet0/1 is up,  line protocol is up  (connected)
  Hardware is Lance,  address is 0030. f279. d401 (bia 0030. f279. d401)
  MTU 1500 bytes, BW 100000 kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set  (10 sac)
  Full-duplex, 100Mb/s
  input  flow-control is off,  output  flow-control is off
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:fifo
  Output queue:0/40  (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

【问题 2】

管理员发现当关闭交换机 Switch2 的 Fa0/2 端口时，Fa0/1 端口指示灯过一段时间后显示正常，请问这是什么原因？Fa0/1 端口经过了哪些状态转换？

【问题 3】

交换机 Switch2 和 Switch3 中都创建了 VLAN，但管理员发现 PC1 主机可以 PING

通 PC2 主机，查看 Switch2 中 VLAN 信息如下所示，请问故障原因是什么？如何修改配置？

```
Switch#show vlan

VLAN  name                  Status    Ports
----  --------------------  --------  ----------------------------------
1     default               active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                      Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                      Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                      Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                      Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                      Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                      Gig1/1, Gig1/2
3    student                active
5    teacher                active
1002 fddi-default           active
1003 token-ring-default     active
1004 fddinet-default        active
1005 trnet-default          active

VLAN Type  SAID   MTU  Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----  ----   ---- ----   ----   ----     ---- ----     ----   ------
1    enet  100001 1500 -      -      -        -    -        0      0
3    enet  100003 1500 -      -      -        -    -        0      0
5    enet  100005 1500 -      -      -        -    -        0      0
```

【问题 4】

管理员发现同属于 VLAN3 的 PC1 和 PC4 主机，以及同属于 VLAN5 的 PC2 和 PC3 主机间不能 PING 通，交换机 Switch2 中的 VLAN 信息和 Switch3 中 VLAN 信息如下所示，请问故障原因是什么？如何修改配置？

```
Switch2#show vlan br

VLAN  Name                          Status   Ports
----  ----------------------------  -------  ---------------------------
1     default                       active   Fa0/1, Fa0/5, Fa0/6, Fa0/7
                                             Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                             Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                             Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                             Fa0/20, Fa0/21, Fa0/22, Fs0/23
                                             Fa0/24, Gig1/1, Gig1/2
```

```
3    student                      active   Fa0/3
5    teacher                      active   Fa0/4
Switch3#show vlan brief

VLAN  Name                        Status   Ports
----  -------------------------   -------  ----------------------------------
1     default                     active   Fa0/1, Fa0/2, Fa0/5, Fa0/6
                                           Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                           Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                           Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                           Fa0/23, Fa0/24, Gig1/1, Gig1/2
3     student                     active   Fa0/3
5     teacher                     active   Fa0/4
```

【问题 5】

管理员发现 STP 协议收敛速度比较慢，请问如何解决？

1. 案例分析

迅速定位并排除网络故障是网络规划师必须具备的能力之一，本案例主要是考查以下知识点。

（1）生成树协议。生成树（Spanning Tree）协议是一种链路管理协议，它为网络提供路径冗余，同时防止产生环路。为使以太网更好地工作，两个工作站之间只能有一条活动路径。网络环路的产生有多种原因，最常见的一种是链路或设备的冗余，为了防止出现一条链路或一台交换机的单点失效问题，在网络建设时往往部署有冗余的链路和交换机。

生成树协议允许网桥之间相互通信以发现网络物理环路。该协议定义了一种算法，网桥能够使用它创建无环路（Loop-Free）的逻辑拓扑结构。换句话说，STP 创建了一个由无环路树叶和树枝构成的树结构，其跨越了整个第二层网络。

生成树协议操作对终端站透明，也就是说，终端站并不知道它们自己是否连接在单个局域网段或多网段中。当有两个交换机同时连接相同的计算机网段时，生成树协议可以允许两台交换机之间相互交换信息，这样只需要其中一个交换机处理该网段计算机之间发送的信息。

交换机之间通过桥接协议数据单元（Bridge Protocol Data Unit，BPDU）交换各自状态信息。生成树协议通过发送 BPDU 信息选出网络中根交换机和根节点端口，并为每个网段选出根节点端口和指定端口。

（2）掌握生成树协议中的端口状态知识。交换机上的端口状态分别为关闭、阻塞、侦听、学习和转发状态。

- 关闭状态：Disabled，不收发任何报文，当接口空连接或人为关闭时处于关闭

状态。

- 阻塞状态：Blocking，不转发用户数据，当交换机刚启动时或出现冗余链路时，端口会处于该状态。需要强调的是，端口在 Blocking 状态时接收 BPDU 信息。
- 侦听状态：Listening，不接收用户数据（15s），收发 BPDU，确定网桥及接口角色。
- 学习状态：Learning，不接收用户数据（15s），收发 BPDU，进行地址学习。
- 转发状态：Forwarding，收发用户数据，继续收发 BPDU 和地址学习，维护 STP。

（3）VLAN 工作原理及配置方法。VLAN 也称为虚拟局域网，是指在交换局域网的基础上，构建的可跨越不同网段、不同网络的端到端逻辑网络。一个 VLAN 组成一个逻辑子网，即一个逻辑广播域，它可以覆盖多个网络设备，允许处于不同地理位置的网络用户加入到一个逻辑子网中。

（4）交换机端口模式。交换机端口有两种模式：Access（访问模式）和 Trunk（干线模式）。一般情况下，处于访问模式的接口只属于一个 VLAN，默认情况下，所有的端口都属于 VLAN 1。访问模式用于与计算机相连，当需要支持跨交换机的 VLAN 时，一般在交换机之间采用干线模式，干线链路上可以传输多个 VLAN 的帧。

处于访问模式的端口收发数据时，不含 VLAN 标识。具有相同 VLAN 号的端口在同一个广播域中。处于干线模式的端口收发数据时，包含 VLAN 标识，除了 Native VLAN 之外。

（5）快速生成树协议。在 IEEE 802.1w 中所界定的快速生成树协议（RSTP）是对在 IEEE 802.1d 中所界定的生成树协议的一种发展。它可以在拓扑发生改变后提供更快的生成树集合，并且能够向局域网或桥接网络提供非循环的网络拓扑。标准的 STP 协议一般在拓扑结构发生变化的 30~50s 后达到稳定状态，而 RSTP 协议一般响应拓扑变化所需的时间是 1s。

RSTP 可以明确区分端口状态（是转发还是阻塞流量）和端口作用（它在拓扑结构中是否扮演了有效的角色）。除了对根端口和 802.1d 中遗留的指定端口进行了定义之外，还说明了两种新的端口状态：一是备份端口 Backup，它提供了连接某局域网网段的备用路径；二是替代端口 Alternate，它为当前根端口所提供的连接根桥路径提供了替代路径。

2．案例参考答案

（1）生成树协议是网络第二层设备的基础协议之一，它通过分布式计算使得网络活动拓扑为树型结构，从而有效地防止了网络中回路的出现，避免了由于帧的无限循环和重复接收所导致网络风暴的发生。根据生成树协议，交换机 Switch2 的 Fa0/1 端口处于 Blocking 状态。可以用 show spanning-tree 命令查看 STP 相关信息，如图 6-6 所示。

（2）当关闭 Switch2 的 Fa0/2 端口后，交换机通过 BPDU 学习到这一端口变化，运行生成树算法重新计算 spanning-tree。这时网络已经不存在冗余路径，Fa0/1 端口应变化为 Forwarding 状态。

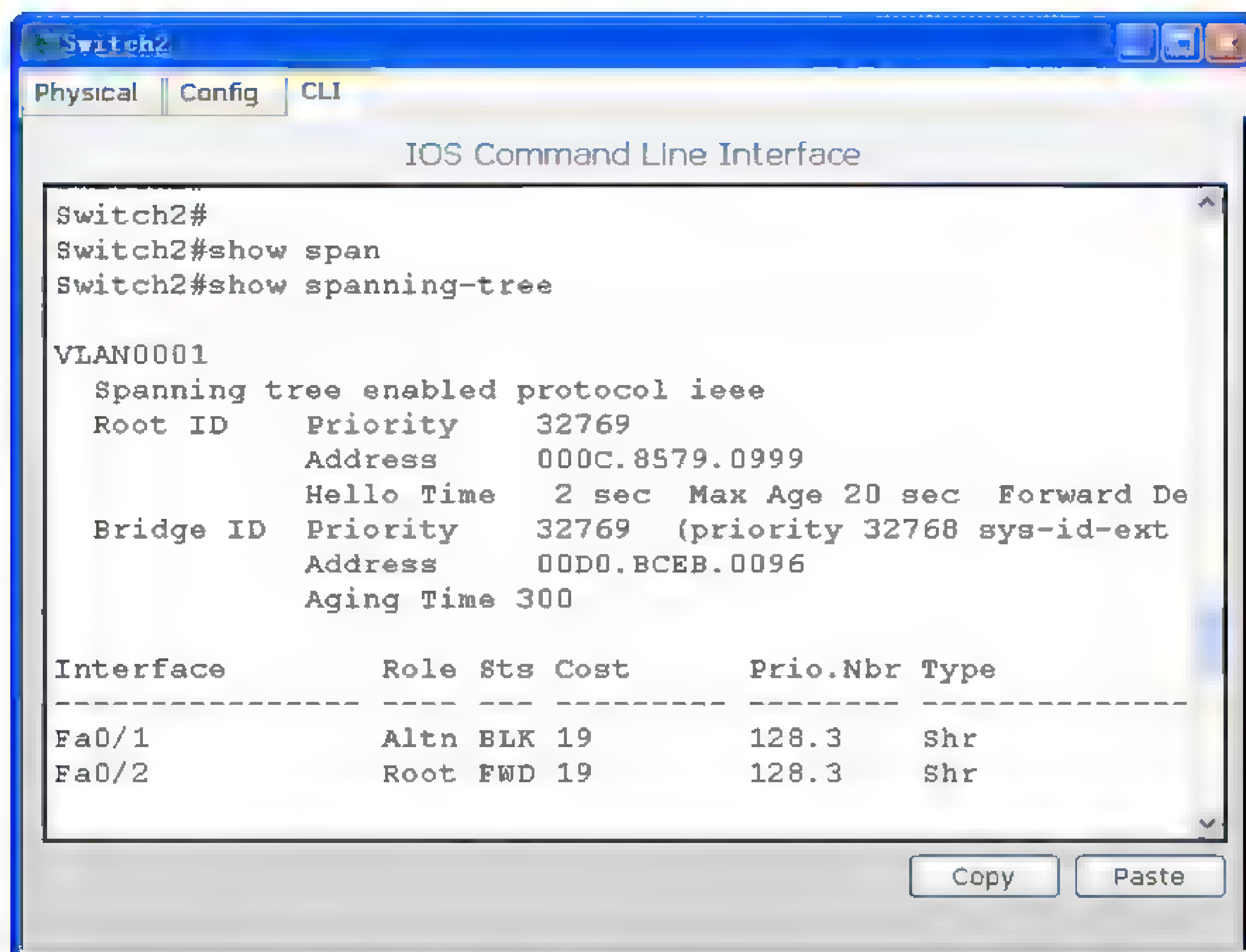


图 6-6 查看 STP 相关信息

Fa0/1 端口经过了 Blocking→Listening→Learning→Forwarding 状态转换。

（3）从显示的交换机 VLAN 信息可以看出，Switch2 中划分了 VLAN 3 和 VLAN 5，但 PC1 连接的端口 Fa0/3 和 PC2 连接的端口 Fa0/4 都还是属于 VLAN 1，没有划分到相应的 VLAN 中。因此，应执行以下配置命令：

```
Switch2(config-if)#int fa0/3
Switch2(config-if)#switchport access vlan 3
Switch2(config-if)#int fa0/4
Switch2(config-if)#switchport access vlan 4
```

（4）根据前面的分析，我们知道在配置跨交换机的多 VLAN 网络时，应把交换机之间的链路设置为干线模式。从显示的 VLAN 信息可以发现，PC 所连接的端口都已划分到相应的 VLAN 中。关键原因是 Switch2 和 Switch3 之间的连接端口没有配置为 Trunk 模式。因此，在两台交换机上应执行以下配置命令：

```
Switch(config-if)#int fa0/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk encapsulation dot1q
```

（5）针对该问题，可以采用快速生成树协议。快速生成树和生成树的区别在于它的

桥协议数据单元的传输是多向的，而且在特定的条件下能将它的某些端口快速地置为转发状态，从而能在几秒的时间内形成稳定的活动拓扑。快速生成树协议定义了 9 个状态机，其中网桥状态机 1 个，端口状态机 8 个。这些状态机相互协作，共同构成了快速生成树协议的理论基础。

RSTP 协议针对 STP 收敛速度慢的问题，对 STP 协议做了一些改进。RSTP 当网络拓扑发生变化时，不像 STP 需要经过 30s 才能从 Blocking 状态转为 Forwarding 状态，大大提高了网络的收敛速度。

第 7 章　网络规划设计论文

7.1　大纲中的要求

《网络规划设计师考试大纲》中，要求考生根据试卷上给出的若干个论文题目，选择其中一个题目，按照规定的要求撰写论文。论文可能涉及的内容极其广泛，主要有网络技术应用与对比分析、网络技术应用对应用系统建设的影响、专用网络设计思路、下一代网络技术分析等主要论题方向，这几个方向又分为若干个子内容。

7.2　论文考试难的原因及其对策

论文写作部分相对于其他部分来说要难些。因为论文写作是对应考者综合能力的检测，而应考者往往因为以下这些原因使得综合能力比较欠缺。

（1）考试范围太广，许多知识没有接触过。

（2）技术方面掌握不扎实，基础不牢。

（3）没有从事过网络规划设计。

（4）缺乏网络规划设计项目实战经验。

（5）长期从事某一个方面的工作，很少从事全面的网络规划设计综合性的工作。

（6）有项目经验但论文写作水平有限，无法准确完整地表达自己的观点。

（7）对考试的论文写作要求不了解。

对于这些问题，要想考试过关，需要注意以下几点。

（1）要尽量以充裕的时间来应考。

（2）要熟悉考试论文的写作格式及注意事项。

（3）掌握一定的论文写作技巧。

（4）需要阅读大量的资料来充实自己。

（5）在考试之前作适当的练习。

当然，如果读者网络规划设计方面的项目经验十分丰富，可以把重点放在锻炼写作技巧上来。

7.3　论文的格式与写作技巧

7.3.1　格式要求

网络规划设计师的论文不同于在学术杂志上发表的学术论文，也不同于学校的毕业论文，它主要是对网络规划设计中某些方面的技术和项目表达自己的观点、思路和解决策略等。因此在格式上的要求也比较简单。

论文书写要注意以下的要求。

（1）达到篇幅要求。

（2）不要在论文中出现过多的图表，尽量用文字表述。

（3）尽量保持卷面整洁，如果确实需要划掉文字，在字上划一横线即可。

（4）不必写关键词。

7.3.2　写作进度把握

论文的写作时间只有 90 分钟，要在很短的时间里写出一篇高质量的论文确属不易，需要考生有较为丰富的理论和实践知识的积累。当然也不必害怕，因为这还是有章可循的。这里建议的时间分配如下。

（1）通读论题，选定论题（5 分钟）。

（2）构思论文，写论文提纲（10 分钟）。

（3）论文写作（65 分钟）。

（4）复查论文（10 分钟）。

下面按写作步骤详细解说。

7.3.3　论文选题

论文写作前，先把几个论文试题快速通览。为了照顾大多数考生的情况，论文题目会比较宽泛。选择自己最容易发挥，最擅长的方向的论题。论文题目选定后就不要犹豫，中途换题会浪费很多时间。

7.3.4　论文提纲

选定论题后不要急于动笔直接在答题纸上写作。因为直接写作很难有一个整体的思路，而且在写作的过程中可能会因涂改而使得卷面不整洁，影响评卷人的心理。也不提倡在草稿纸上书写论文再抄至论文答题纸上，因为考试的时间本来就十分有限，抄写论文也需要较多时间。不妨先花点时间理理写作的思路，在草稿纸上写出论文的提纲，所谓“磨刀不误砍柴工”。

7.3.5 正文写作

有了提纲，写正文就轻松多了。正文可采用“总—分—总”式，即文章开头提出中心思想，再分述论点，最后在结尾处做出总结；也可用“提出问题—分析问题—解决问题”的逐步深入的方法。写作时注意以下几个方面的技巧。

（1）看清题目中给出的要点，抓住要点进行论述；内容要切题，紧紧围绕着试题指定的范围写作，不要离题发挥写过多无关的内容，不要给人以拼凑论文的感觉。

（2）理论联系实际，要有充实的具体内容，切忌空谈理论。

（3）论点要正确，合乎工程实践的实际情况。

（4）要注重逻辑性和条理性。有事实作为依据，力求要有说服力，条理清晰，前后呼应，不能够出现有自相矛盾的情况。

（5）要突出是你自己亲身经历完成的，语气要自信，要有自己的观点与见解。

（6）遇到过的问题和解决这些问题的措施或策略应当具体化，是很现实可信的。

（7）采取措施的效果，要求比较突出，切实可行。

（8）需要进一步改进的地方和如何进行改进，要求写得比较明确，不能很含糊。

（9）论点清晰，最好每段在开头处或结尾处点明论点。

（10）可采用分条叙述的方式，但不要全文用此方式。

（11）不必列举过多的计算公式。

（12）文章要带有一定的学术性。

7.3.6 复查论文

复查论文主要是检查论文是否通顺、有无遗漏、有无错别字。注意以下几点。

（1）卷面要保持整洁。

（2）格式整齐，字迹工整。

（3）在时间不够的情况下力求写完论文，切忌有头无尾。

7.4 论文范文

[题目]：论信息系统建设的网络规划

网络规划在信息系统建设中占有重要地位，一方面要满足信息系统的应用需求，另一方面受到信息系统覆盖的地理空间范围、资金和其他资源约束；既要满足当前信息系统的需要，又要满足未来发展的需要，即网络规划方案不仅要有实用性，还要有扩展性。

请围绕“信息系统建设的网络规划”论题，依次从以下三个方面进行论述。

1．概要叙述你参与分析设计的信息系统的应用需求以及你在其中所担任的主要工作。

2. 深入论述你参与设计的信息系统网络规划主要涉及哪些方面，这些方面是如何满足信息系统应用需求并且具有实用性和扩展性的？

3. 简要叙述你参与的信息系统的网络规划方案中，除了实用性和扩展性外，方案中还有哪些特性需要考虑？

[范文]

我一直在某 IT 公司从事技术规划和项目实施工作，去年作为项目经理组织实施了某市远程医学教育网络系统平台的建设。

该项目是建立某市远程医学教育网络系统平台，以现有的国际互联网为基础，综合运用卫星网络以及虚拟专网，以市医科大学第一附属医院为中心，向东依托沿海发达城市的医疗资源，向西覆盖全市 14 个市级医院。初步构架市远程医学三级网络系统，即沿海发达城市远程医学中心—市远程医学中心—各市级医院。通过构建这个平台使各市级医院不仅共享本地的医学资源优势，同时共享到沿海发达城市医院的医疗资源。通过远程医学教育、远程医疗咨询（现场诊断咨询）、手术观摩、虚拟手术等多种现代教育手段，实现真正意义的医学资源的联动，造就市高素质的专业医学人才。我作为项目负责人参与了整个项目的应用需求分析、具体技术方案设计及部分子系统模块的研发。

为进行信息系统建设的网络规划，首先需要对系统的网络通信需求进行详细的分析。

（1）地面网络

市远程医学教育网络主要使用单位包括市远程医学中心、各市级医院（医疗机构）以及其他医疗机构及医疗网点，各市级医院（医疗机构）与市指挥中心具备地面宽带通信条件。平时以远程医学教学、远程医疗咨询的应用为主，地面网络具有成本优势。但是地面有线链路节点众多，结构复杂意味着可能发生故障的环节增多，对技术维护和支持的要求增高。因此很难在大范围内对各个网络层次可能的故障点上提供及时有效的故障响应。其他基于地面的无线链路多半也存在中转站的维护问题，所以采用卫星网络作为备份。

（2）卫星网络

一般认为地面线路带宽较高，大数据量信息传送的速度可能较快，但不能忽略的是由许多线路段连接而成的长途地面通信信道速率是由这些线路段中速率最低者所决定的（瓶颈效应），而卫星通信系统不存在这个问题。

市医疗基层单位大多分散在没有地面宽带条件的地区，因此可以利用卫星通信距离远，且不受地面条件限制的优势，为各基层医院建立双向卫星地面站，通过设立在上海的 MCU 交换后与市的 MCU 进行级联。

市远程医学教育网采用的是亚洲四号卫星 Ku 波段卫星数字广播。与以往的 C 波段卫星模拟广播相比，使用较高频率的 Ku 波段及先进的数字压缩技术具有明显的优势。

（3）虚拟专网

虚拟专用网是以公用网络 Internet 为基础，结合隧道封装、认证、加密、访问控制

等多种网络安全技术，为企业总部和分支机构及移动办公人员提供安全网络连通的技术。VPN 的主要目标是建立一种低投入、方便快捷的网络互连方式，替代传统专线连接和拨号连接。本系统的二维医学影像网络系统构建在远程医学教育网络信息平台上，采用的是虚拟专网。

在分析系统网络通信需求的基础上，市远程医学教育网络信息平台设计为：以地面宽带加卫星通信方式为主要通信手段；以流媒体技术、医学影像技术、医学信息交互传输技术于一体；以强化远程医学教育功能、规范远程医学教育流程为主要的设计理念；以 Web 化为核心的技术路线作为本系统平台的总体解决方案。

对于有宽带的用户，采用：双向卫星地面小站+地面宽带：开展远程医疗咨询时，以地面宽带网络为主，以双向卫星作备份。接收远程教育时，通过卫星接收节目，通过地面宽带或卫星备份进行回传。单向卫星地面小站+地面宽带：利用单向卫星广播优势的特点，来接收远程教育系统的教学节目，以地面网络作为回传线路，进行双向交互的远程培训。

对于无宽带的用户，采用双向卫星地面小站。对只需要开展远程教育的，并且不需要进行交互的，采用单向卫星小站。

以市远程中心 MCU 服务器为管理和控制的核心，采用双向通信链路，与沿海发达城市的医学中心（上海等）联网，再通过沿海远程医学中心与省内各医院联网，如上海远程医学中心管理的华山医院、中山医院、瑞金医院等，北京的医学中心管理的北医三院、协和医院等。

可见，信息系统建设的网络规划必须具备以下两点。

（1）信息系统建设的网络规划必须充分保证信息系统的功能实现。该系统是基于计算机地面网络技术、卫星网络技术和多媒体通信技术，建立基于分布开放式的应用系统。整个系统平台由 6 大子系统构成，即远程医学咨询系统、手术直播观摩系统、远程医学教育系统、远程虚拟手术实验系统、视频会议系统和远程电子图书馆。网络规划必须为系统 6 大功能子系统的实现提供网络平台保证。

（2）信息系统建设的网络规划必须充分支撑信息系统关键技术的实施。本系统主要包括 IP 组播技术、计算机集群技术、中间件技术、虚拟现实技术等关键技术。每个关键技术都离不开网络平台的支撑，网络规划必须为这些关键技术的实施提供网络平台保证。

缩 写 词

A/D，Analogue/Digital，模/数变换
ABR，Area Border Router，区域边界路由器
ADSL，Asymmetric Digital Subscriber Line， 非对称 DSL
AF，Assured Forwarding，确保转发
AM，Amplitude Modulation，调幅
AN，Access Network，接入网
ARQ，Automatic Repeat reQuest，检错重发
AS，Autonomous System，自治区域
ASK，Amplitude Shift Keying，幅移键控
ASN.1，Abstract Syntax Notation one，抽象语法标记
ATM，Asynchronous Transfer Mode，异步传输模式
B8ZS，Bipolar with 8-zeros Substitution，双极性 8 零替换码
BB，Bandwidth Broker，带宽代理
BBE，Better than Best-Effort service，优于尽力而为服务
BDT，Bureau of Development of Telecommunication，电信发展局
BE，Best Effort，尽力而为
BER，Basic Encoding Rule，基本编码规则
BES，Best Effort Service，尽力而为服务型
BGAN，Broadband Global Area Network，宽带全球网络
BGP，Border Gateway Protocol，边界网关协议
B-ISDN，Broadband ISDN，宽带 ISDN
BRI，Basic Rate Interface，基本速率接口
CA，Certificate Authority，证书授权中心
CCIR，Consultative Committee of International Radio，国际无线电咨询委员会
CCITT，Consultative Committee on International Telegraph and Telephone，国际电报电话咨询委员会
CD，Committee Draft，委员会草案
CDDI，Copper Distributed Data Interface，铜线分布数据接口
CDMA，Code Division Multiplex Access，码分多址
CE，Custom Edge Router，用户边界路由器

CLS，Control Load Service，受控负载服务型
CM，Cable Modem，电缆调制解调器
COPS，Common Open Policy Service，公共开放策略服务
CRC，Cyclic Redundancy Check，循环冗余校验
CRL，Certificate Revocation Lists，证书废除列表
DDN，Digital Data Network，数字数据网络
DIS，Draft International Standard，国际标准草案
DP，Draft Proposal，建议草案
DRR，Deficit Round-Robin，亏空轮循
DRSVP，Dynamic Resource Reservation Protocol，动态资源预留协议
DS，Differentiated Service，区分服务
DS，Direct Sequencing，直接序列扩频
DSCP，Differentiated Service Code Point，区分服务码点
DSL，Digital Subscriber Lines，数字用户线路
EF，Expedited Forwarding，加速转发
EFD，Expedited Forwarding with Dropping，允许丢失的加速转发
EFS，Encrypting File System，加密文件系统
EGP，External Gateway Protocol，外部网关协议
EPD，Early Packet Discard，早期分组丢弃
ETSI，European Telecommunication Standards Institute，欧洲电信标准协会
FDDI，Fiber Distributed Data Interface，光纤分布数据接口
FDM，Frequency-Division Multiplexing，频分多路复用
FEC，Forwarding Equivalence Class，转发等价类
FH，Frequency Hopping，跳频
FM，Frequency Modulation，调频
FR，Frame Relay，帧中继
FSK，Frequency Shift Keying，频移键控
GLBP，Gateway Load Balancing Protocol，网关负载均衡协议
GPRS，General Packet Radio Service， 通用分组无线业务
GQA，Global QoS Agent，全局服务质量代理
GS，Guaranteed Service，保证服务型
GSM，Global System for Mobile Communication， 全球移动通信系统
HDB3，High-Density Bipolar-3 zeros，三阶高密度双极性码
HDLC，High Level Data Link Control， 高级数据链路控制协议
HFC，Hybrid Fiber/Coax，混合光纤/铜缆

HSRP，Hot Standby Router Protocol，热备份路由器协议
HTTPS，HTTP Over TLS，基于 TLS 的 HTTP 协议
IETF，the Internet Engineering Task Force，因特网工程任务组
IFRB，International Frequency Registration Board，国际频率登记委员会
IGP，Interior Gateway Protocol，内部网关协议
IS，Integrated Service，综合服务
IS，International Standard，国际标准
ISDN，Integrated Service Digital Network， 综合业务数字网
ISO，International Standardization Organization，国际标准化组织
ITU，International Telecommunication Union，国际电信联盟
LBE，Lower than Best Effort，准尽力而为
LC，Lexical Conventions，文字约定
LDP，Label Distribution Protocol，标记分配协议
LQA，Local QoS Agent，归属服务质量代理
LSP，Label Switched Path，标记交换路径
LSR，Label Switching Router，标记交换路由器
MIB，Management Information Base，管理信息库
MPLS，Multiprotocol Label Switching，多协议标签交换
MRSVP，Resource Reservation Protocol with Mobile Hosts，移动资源预留协议
MSTP，Multi-service Transport Platform，多业务传送平台
MTBF，Mean Time Between Failure，平均无故障时间
NBNS，NetBIOS Name Server，NetBIOS 名字服务器
NIC，Network Information Center，网络信息中心
N-ISDN，Narrow ISDN，窄带 ISDN
NMF，Network Management Forum，网络管理论坛
NMS，Network Management System，网络管理系统
NOC，Network Operation Center，网络运行中心
ODP，Open Distributed Processing，开放分布式处理
OSPF，Open Shortest Path First，最短路径优先协议
P2P，Point-to-Point，点对点/对等网
PE，Provider Edge Router，运营商边界路由器
PDH，Plesiochronous Digital Hierarchy，准同步数字系列
PHB，Per-Hop-Behavior，逐跳行为
PHB-I，Interoperability PHB group，协同 PHB 组
PKI，Public Key Infrastructure，公钥基础设施

PM，Phase Modulation，调相
POE，Power over Ethernet，以太网供电
PON，Passive Optical Network，无源光网络
PPD，Partial Packet Discard，部分分组丢弃
PPS，Packets Per Second，数据包每秒
PRI，Primary Rate Interface，基群速率接口
PSK，Phase Shift Keying，相移键控
PSTN，Public Switch Telephone Network，公用交换电话网
PVC，Permanent Virtual Circuit，永久虚连接
QAM，Quadrature Amplitude Modulation，正交振幅调制
QAMP，Quantitative Assured Media Playback service，定量确保的多媒体播放服务
QoS，Quality of Service，服务质量
RA，Registration Authority，注册机构
RED，Random Early Discard，随机早期丢弃
RFC，Request For Comments，请求注解
RMON，Remote network MONitoring，远程网络监视
RMS，Resource Management System，资源管理系统
RS，Radicommunication Sector，无线电通信部门
RSTP，Rapid Spanning-Tree Protocol，快速生成树协议
RSVP，Resource ReSerVation Protocol，资源预留协议
RTT，Round-Trip Time，往返时延
SBM，Subnet Bandwidth Management，子网带宽管理
SCFQ，Self Clocked Fair Queuing，自时钟公平排队
SDH，Synchronous Digital Hierarchy，光同步数字传输网
SET，Secure Electronic Transaction，安全电子交易
SLA，Service Level Agreement，服务等级协议
SLS，Service Level Specification，服务等级规范
SMI，Structure of Management Information，管理信息结构
SNMP，Simple Network Management Protocol，简单网络管理协议
SONET，Synchronous Optical Network，同步光纤网
SSL，Security Socket Layer，安全套接层协议
STDM，Statistic Time-Division Multiplexing，统计时分多路复用
STP，Shielded Twisted Pair，屏蔽双绞线
STP，Spanning-Tree Protocol，生成树协议
SVC，Switched Virtual Circuit，交换虚连接

TC，Technical Committee，技术委员会

TCA，Traffic Conditioning Agreement，流量调节协议

TCS，Traffic Conditioning Specification，流量调节规范

TDM，Time-Division Multiplexing，时分多路复用

TDS，Telecommunication Development Sector，电信发展部门

TD-SCDMA，Time Division-Synchronous Code Division Multiple Access，时分同步的码分多址

TH，Time Hopping，跳时

TLS，Transport Layer Security Protocol，安全传输层协议

TMS，Transport Management System，传输管理系统

TOM，Telecom Operations Map，电信运营图

TPDU，Transport Protocol Data Unit，传输协议数据单元

TPH，Transactions Per Hour，事务处理数每小时

TPS，Transactions Per Second，事务处理数每秒

TR，Technical Report，技术报告

TRIB，Throughput Rate of Information Byte，信息比特吞吐率

TSAP，Transport Service Access Point，传输服务访问点

TSS，Telecommunication Standardization Sector，电信标准化部门

UTP，Unshielded Twisted Pair，非屏蔽双绞线

VC，Virtual Circuit，虚电路

VLAN，Virtual Local Area Network，虚拟局域网

VPN，Virtual Private Network，虚拟专用网

VRRP，Virtual Router Redundancy Protocol，虚拟路由器冗余协议

VSAT，Very Small Aperture Terminal，甚小口径卫星终端站

WAN，Wide Area Network，广域网

WBM，Web-Based Management，基于 Web 的网络管理

WDM，Wavelength-Division Multiplexing，波分多路复用

WFQ，Weighted Fair Queuing，加权公平排队

Wi-Fi，Wireless Fidelity，无线保真

WiMAX，Worldwide Interoperability for Microwave Access，微波接入互操作性

WLAN，Wireless Local Area Network，无线局域网

WRR，Weighted Round-Robin，权重轮询

参 考 文 献

[1] 冯建和. ADSL 宽带接入技术及应用. 北京：人民邮电出版社，2002.
[2] 黄永峰. IP 网络多媒体通信技术. 北京：人民邮电出版社，2003.
[3] Larry L.Peterson，Bruce S.Davie.《计算机网络系统方法》，北京：机械工业出版社，2005.
[4] 刘韵洁，张云勇，张智江. 下一代网络服务技术. 北京：电子工业出版社，2005.
[5] 王健全等. 城域 MSTP 技术. 北京：机械工业出版社，2005.
[6] 王卫红，李晓明. 计算机网络与互联网. 北京：机械工业出版社，2009.
[7] 吴功宜. 计算机网络高级教程. 北京：清华大学出版社，2007.
[8] William Stallings 编著. 齐望东，薛卫娟，傅麒麟等译. 高速网络与互联网——性能与服务质量. 北京：电子工业出版社，2003.
[9] 肖明. 计算机网络. 北京：机械工业出版社，2007.
[10] 谢希仁. 计算机网络（第 5 版）. 北京：电子工业出版社，2008.
[11] 胡谷雨. 网络管理技术教程. 北京：北京希望电子出版社，2002.
[12] Mani Subramanian 编著. 王松，周靖，孟纯城译. 网络管理原理与实践. 北京：高等教育出版社，2003.
[13] 张沪寅，吴黎兵，吕慧等. 计算机网络管理实用教程. 武汉：武汉大学出版社，2005.
[14] 张国鸣，唐树才，薛刚逊. 网络管理实用技术. 北京：清华大学出版社，2002.
[15] 陈明.计算机网络设计教程（第 2 版）. 北京：清华大学出版社，2008.
[16] 陈向阳，肖迎元，陈晓明，余小鹏. 网络工程规划与设计. 北京：清华大学出版社，2007.
[17] 段水福，历晓华，段炼. 无线局域网（WLAN）设计与实现. 浙江：浙江大学出版社，2007.
[18] Priscilla Openheimer. 自底向下网络设计（第 2 版）. 北京：人民邮电出版社，2005.
[19] 杨丰瑞，刘辉，张勇. 通信网络规划. 北京：人民邮电出版社，2005.
[20] 杨威，王云，刘景宜.网络工程设计与系统集成. 北京：人民邮电出版社，2007.
[21] 杨卫东. 网络系统集成与工程设计（第 2 版）. 北京：科学出版社，2005.
[22] 易建勋. 计算机网络设计. 北京：人民邮电出版社，2007.
[23] 韩一石，强则煊，许国良. 现代光纤通信技术. 北京：科学出版社，2005.
[24] 拉奥 • 博伊科维奇 • 米洛瓦诺维奇. 多媒体通信系统：技术、标准及网络. 北京：清华大学出版社，2004.
[25] 穆道生. 现代光纤通信系统. 北京：科学出版社，2005.
[26] 任海兰，刘德明.光通信信号处理. 北京：电子工业出版社，2006.
[27] 索红光. 现代通信技术概论（第 2 版）. 北京：国防工业出版社，2005.
[28] 王秉钧，王少勇. 光纤通信系统. 北京：电子工业出版社，2004.
[29] William A.Shay. 数据通信与网络教程. 北京：机械工业出版社，2000.
[30] 鲜继清，张德民等. 现代通信系统. 西安：西安电子科技大学出版社，2003.
[31] 徐家凯，沈庆宏等. 通信原理教程. 北京：科学出版社，2007.
[32] 杨世平，张引发，邓大鹏，何渊. SDH 光同步数字传输设备与工程应用. 北京：人民邮电出版社，2004.
[33] 周卫东，罗国民，朱勇等. 现代传输与交换技术. 北京：国防工业出版社，2003.

[34] 张德纯，王兴亮等. 现代通信理论与技术导论. 西安：西安电子科技大学出版社，2004.
[35] 史兴键. 安全强审计模型研究. 西安：西北工业大学：博士学位论文，2006.
[36] 陈珍成. 信息安全管理体系审核指南. 北京：中国标准出版社，2007.
[37] 范红，冯登国，吴亚非. 信息安全风险评估方法与应用. 北京：清华大学出版社，2006.
[38] 范红. 信息安全风险评估规范国家标准理解与实施. 北京：中国标准出版社，2008.
[39] 胡道元，闵京华. 网络安全. 北京：清华大学出版社，2004.
[40] 黄传河，杜瑞颖等. 网络安全. 武汉：武汉大学出版社，2004.
[41] Mark Osborne 编著，周广辉等译. 信息安全管理之道. 北京：中国水利水电出版社，2008.
[42] 王春东. 信息安全管理. 武汉：武汉大学出版社，2008.
[43] Michael E. Whitman, Herbert J. Mattord 著，徐焱译. 信息安全原理. 北京：清华大学出版社，2004.
[44] 吴世忠，陈晓桦等. 信息安全测评认证理论与实践. 北京：北京中电电子出版社；合肥：中国科技大学出版社，2006.
[45] 吴亚非，李新友，禄凯. 信息安全风险评估. 北京：清华大学出版社，2007.
[46] 徐国爱，彭俊好，张淼. 信息安全管理. 北京：北京邮电大学出版社，2008.
[47] 赵战生，谢宗晓. 信息安全风险评估：概念、方法和实践. 北京：中国标准出版社，2007.
[48] RFC2246，The TLS Protocol Version 1.0， http：//www.ietf.org/rfc/rfc2246.txt.
[49] RFC2459，Internet X.509 Public Key Infrastructure Certificate and CRL Profilehttp：//www.ietf.org/rfc/rfc2459.txt.
[50] RFC2818，HTTP Over TLS， http：//www.ietf.org/rfc/rfc2818.txt.
[51] RFC3281，An Internet Attribute Certificate Profile for Authorization, http：//www.ietf.org/rfc/rfc3281.txt.